# On the Efficiency of Classical and Quantum Secure Function Evaluation

Severin Winkler and Jürg Wullschleger

***Abstract*—We provide bounds on the efficiency of secure one-sided output two-party computation of arbitrary finite functions from trusted distributed randomness in the statistical case. From these results we derive bounds on the efficiency of protocols that use different variants of OT as a black-box. When applied to implementations of OT, these bounds generalize most known results to the statistical case. Our results hold in particular for transformations between a finite number of primitives and for any error. In the second part we study the efficiency of quantum protocols implementing OT. While most classical lower bounds for perfectly secure reductions of OT to distributed randomness still hold in the quantum setting, we present a statistically secure protocol that violates these bounds by an arbitrarily large factor. We then prove a weaker lower bound that does hold in the statistical quantum setting and implies that even quantum protocols cannot extend OT. Finally, we present two lower bounds for reductions of OT to commitments and a protocol based on string commitments that is optimal with respect to both of these bounds.**

***Index Terms*—Unconditional security, oblivious transfer, lower bounds, two-party computation, quantum cryptography.**

## I. Introduction

Secure multi-party computation allows two or more distrustful players to jointly compute a function of their inputs in a secure way [2]. Security here means that the players compute the value of the function correctly without learning more than what they can derive from their own input and output.

A primitive of central importance in secure multi-party computation is *oblivious transfer* (OT). In particular, OT is sufficient to execute any two-party computation securely [3], [4] and OT can be precomputed offline, i.e., before the actual inputs to the computation are available, and converted into OTs later. The original form of OT ($(\frac{1}{2})$-RabinOT$^1$) has been introduced by Rabin in [5]. It allows a sender to send a bit $x$, which the receiver will get with probability $\frac{1}{2}$, while the sender does not learn whether the message has arrived or not. Another variant of OT, called one-out-of-two bit-OT ($\binom{2}{1}$-OT$^1$) was defined in [6]. Here, the sender has two input bits $x_0$ and $x_1$. The receiver gives as input a choice bit $c$ and receives $x_c$ without learning $x_{1-c}$. The sender gets no information about the choice bit $c$. Other important variants of OT are $\binom{n}{t}$-OT$^k$ where the inputs are strings of $k$ bits and the receiver can choose $t < n$ out of $n$ secrets and $(p)$-RabinOT$^k$ where the inputs are strings of $k$ bits and the erasure probability is $p \in [0, 1]$.

If the players have access to noiseless classical or quantum communication only, it is impossible to implement information-theoretically secure OT, i.e. secure against an adversary with unlimited computing power. The primitives $(p)$-RabinOT$^k$ and $\binom{2}{1}$-OT$^1$ are equally powerful [7], i.e., one can be implemented from the other. Numerous reductions of $\binom{n}{1}$-OT$^k$ to $\binom{2}{1}$-OT$^{k'}$ are known [8], [9], [10], [11], [12]. There has also been a lot of interest in reductions of OT to weaker primitives. For example, OT can be realized from noisy channels [13], [14], [15], [16], noisy correlations [17], [18], or weak variants of oblivious transfer [13], [19], [20], [21], [22], [23].

In the quantum setting, OT can be implemented from black-box commitments [24], [25], [26], [27]; this reduction is impossible in the classical setting[1].

Given these positive results it is natural to ask how efficient such reductions can be in principle, i.e., how many instances of a given primitive are needed to implement OT.

### A. Previous Results

Several lower bounds for OT reductions are known. The earliest impossibility result for information-theoretically secure reductions of OT [28] shows that the number of $\binom{2}{1}$-OT$^1$ cannot be *extended*, i.e., there does not exist a protocol using $n$ instances of $\binom{2}{1}$-OT$^1$ that perfectly implements $m > n$ instances. Lower bounds on the number of instances of OT needed to perfectly implement other variants of OT have been presented in [11] (see also [29]). These bounds have been strengthened and generalized to secure sampling of arbitrary two-party distributions in [12], [30], [31], [32]. These bounds apply to the semi-honest model (where dishonest players follow the protocol, but try to gain additional information from the transcript of the computation) and in the case of implementations of OT also to the malicious model (where dishonest players behave arbitrarily). In the malicious model these bounds can be improved [33]. Lower bounds on the number of ANDs needed to implement general functions have been presented in [34].

These results only consider *perfect* protocols and do not give much insight into the case of statistical implementations. As pointed out in [33], their result *only* applies to the perfect case, because there is a statistically secure protocol that is more efficient [35]. There can be a large gap between the efficiency of perfect and statistical protocols, as shown in [34]:

A preliminary version of this work appeared in [1].

S. Winkler is with the Computer Science Department, ETH Zürich, CH-8092 Zürich, Switzerland (e-mail: swinkler@ethz.ch)

J. Wullschleger is with Université de Montréal and McGill University, Montréal (Québec), Canada

[1] The existence of a classical reduction of OT to bit commitment in the malicious model would imply a semi-honest OT protocol from a communication channel only.

The number of OTs needed to compute the equality function is exponentially bigger in the perfect case than in the statistical case. Therefore, it is not true in general that a bound in the perfect case implies a similar bound in the statistical case.

So far very little is known in the statistical case. In [36] a proof sketch of a lower bound for statistical implementations of $\binom{2}{1}$-$\mathsf{OT}^k$ has been presented. However, this result only holds in the asymptotic case, where the number $n$ of resource primitives goes to infinity and the error goes to zero as $n$ goes to infinity. In [34] a non-asymptotic lower bound on the number of ANDs needed for one-sided secure computation of arbitrary functions with *Boolean* output has been shown. This result directly implies lower bounds for protocols that use $\binom{n}{t}$-$\mathsf{OT}^k$ as a black-box. However, besides being restricted to Boolean-valued functions this result is not strong enough to show optimality of several known reductions and it does not provide bounds for reductions to randomized primitives such as $(\frac{1}{2})$-$\mathsf{RabinOT}^1$. The impossibility results for perfectly secure implementations of randomized two-party primitives of [31], [32] should also generalize to the case of a small statistical error according to the authors.

In the quantum setting almost all known negative results show that a certain primitive is impossible to implement from scratch. Commitment has been shown to be impossible in the quantum setting in [37], [38]. Using a similar proof, it has been shown in [39] that general one-sided two-party computation and in particular oblivious transfer are also impossible to implement securely in the quantum setting.

The only lower bounds for quantum protocols where the players have access to resource primitives (such as different variants of OT) have been presented in [40], where Theorem 4.7 shows that important lower bounds for classical protocols also apply to *perfectly* secure quantum reductions.

### B. Contributions

In Section III we consider statistically secure protocols that compute a function between two parties from trusted randomness distributed to the players. We provide two bounds on the efficiency of such reductions — in terms of the conditional Shannon entropy and the mutual information of the randomness — that allow us in particular to derive bounds on the minimal number of $\binom{n}{1}$-$\mathsf{OT}^k$ or $(p)$-$\mathsf{RabinOT}^k$ needed to compute a general function securely. Our results hold in the non-asymptotic regime, i.e., we consider a finite number of resource primitives and our results hold for *any* error.

We will use the formalism of smooth entropies to show that one of these two bounds can be generalized to a bound in terms of the conditional min-entropy. This leads to tighter bounds in many cases and to arbitrarily better bounds for some reductions.

In Section III-A we provide an additional bound for the special case of statistical implementations of $\binom{n}{1}$-$\mathsf{OT}^k$ in the semi-honest model. Lower bounds for implementations of OT in the semi-honest model imply similar bounds in the malicious model (cf. Section III-E and Appendix A). The bounds for implementations of $\binom{n}{1}$-$\mathsf{OT}^k$ (Theorem 4) imply the following corollary that gives a general bound on the conversion rate between different variants of OT.

*Corollary 1:* For any reduction that implements $M$ instances of $\binom{N}{1}$-$\mathsf{OT}^K$ from $m$ instances of $\binom{n}{1}$-$\mathsf{OT}^k$ in the semi-honest model with an error of at most $\varepsilon$, we have

$$\frac{m}{M} \geq \max\left(\frac{(N-1)K}{(n-1)k}, \frac{K}{k}, \frac{\log N}{\log n}\right) - 7NK \cdot (\varepsilon + h(\varepsilon)) .$$

Corollary 1 generalizes the lower bounds from [11], [12], [30] to the statistical case and is strictly stronger than the impossibility bounds from [36]. If we let $M = m + 1$, $N = n = 2$ and $K = k = 1$, we obtain a stronger version of Theorem 3 from [28] which states that OT cannot be extended. Note that the impossibility results for perfectly secure implementations of randomized two-party primitives of [31], [32] deliver stronger bounds in general (cf. Example 4.1 in [32]), and according to the authors these results should also generalize to the case of a small statistical error. However, in contrast to our results they are restricted to randomized primitives only and do not apply to general two-party functions.

Our lower bounds show that the following protocols are (close to) optimal in the sense that they use the minimal number of instances of the given primitive.

- The protocol in [41], [11] which uses $\frac{N-1}{n-1}$ instances of $\binom{n}{1}$-$\mathsf{OT}^k$ to implement $\binom{N}{1}$-$\mathsf{OT}^k$ is optimal.
- The protocol in [12] which uses $t$ instances of $\binom{n}{1}$-$\mathsf{OT}^{kn^{t-1}}$ to implement $\binom{n^t}{1}$-$\mathsf{OT}^k$ is optimal.
- In the semi-honest model, the trivial protocol that implements $\binom{2}{1}$-$\mathsf{OT}^k$ from $k$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ is optimal. In the malicious case, the protocol in [35] uses asymptotically (as $k$ goes to infinity) the same amount of instances and is therefore asymptotically optimal.
- The protocol in [42] that implements $\binom{2}{1}$-$\mathsf{OT}^k$ from $(\frac{1}{2})$-$\mathsf{RabinOT}^1$ in the malicious model is asymptotically optimal.

While previous results suggest that quantum protocols are not more efficient than classical protocols for reductions between different variants of oblivious transfer, we present in Section IV a statistically secure protocol that violates the classical bounds and the bound for perfectly secure quantum protocols by an arbitrarily large factor. More precisely, we prove that, in the quantum setting, string oblivious transfer can be reversed much more efficiently than by any classical protocol. We show that a weaker lower bound for quantum reductions holds also for quantum protocols in the statistical setting (Theorem 8). This result implies in particular that quantum protocols cannot extend oblivious transfer, i.e., there exists a constant $c > 0$ such that any quantum reduction of $m + 1$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ to $m$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ must have an error of at least $\frac{c}{m}$. Finally, we also derive a lower bound on the number of commitments (Theorem 10) and on the total number of bits the players need to commit to (Theorem 7) in any $\varepsilon$-secure implementation of $\binom{2}{1}$-$\mathsf{OT}^k$ from commitments.

*Corollary 2:* A protocol that implements $\binom{2}{1}$-$\mathsf{OT}^k$, using commitments only, with an error of at most $0 < \varepsilon \leq 0.002$ must use at least $\log(1/\varepsilon) - 6$ individual commitments and needs to commit to at least $(1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon})$ bits in total.

## II. Preliminaries

We denote the distribution of a random variable $X$ by $P_X(x)$. Given the distribution $P_{XY}$ over $\mathcal{X} \times \mathcal{Y}$, the marginal distribution is denoted by $P_X(x) := \sum_{y \in \mathcal{Y}} P_{XY}(x,y)$. For every $y \in \mathcal{Y}$ with $P_Y(y) > 0$, the conditional distribution $P_{X|Y}(x,y) := P_{XY}(x,y)/P_Y(y)$ over $\mathcal{X} \times \mathcal{Y}$ defines a distribution $P_{X|Y=y}$ with $P_{X|Y=y}(x) = P_{X|Y}(x,y)$ over $\mathcal{X}$. Given an event $\Omega$ and random variables $X$ and $Y$ with a joint distribution $P_{\Omega XY}$, we use the notation $P_{X\Omega|Y=y}$ for the sub-normalized distribution with $P_{X\Omega|Y=y}(x) := P_{X|Y=y}(x) P_{\Omega|X=x,Y=y}(1)$ . We will also use the shorthand notation $P_{\Omega|X=x}$ to denote the probability $P_{\Omega|X=x}(1)$. We use the convention that $P_{X\Omega|Y=y}(x) = 0$ if $P_Y(y) = 0$.

The *statistical distance* between the distributions $P_X$ and $P_{X'}$ over the domain $\mathcal{X}$ is defined as the maximum, over all (inefficient) distinguishers $\delta : \mathcal{X} \to \{0,1\}$, of the distinguishing advantage:

$$\mathrm{D}(P_X, P_{X'}) := \max_{\delta} \mid \Pr[\delta(X) = 1] - \Pr[\delta(X') = 1] \mid .$$

If $\mathrm{D}(P_X, P_{X'}) \leq \varepsilon$, we may also say that $P_X$ is $\varepsilon$-close to $P_{X'}$. The support of a distribution $P_X$ over $\mathcal{X}$ is defined as $\text{supp}\,(P_X) := \{x \in \mathcal{X} : \; P_X(x) > 0\}$. If $x = (x_1, \ldots, x_n)$ and $T := \{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$, then $x_T$ denotes the sub-string $(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$ of $x$. If $x, y \in \{0,1\}^n$, then $x \oplus y$ denotes the bitwise XOR of $x$ and $y$.

### A. Information Theory

The *conditional Shannon entropy* of $X$ given $Y$ is defined as[2]

$$H(X|Y) := - \sum_{(x,y) \in \text{supp}\,(P_{XY})} P_{XY}(x,y) \log P_{X|Y}(x,y) .$$

The *mutual information* of $X$ and $Y$ given $Z$ is defined as

$$I(X;Y|Z) := H(X|Z) - H(X|YZ) .$$

We use the notation

$$h(p) := -p \log p - (1-p) \log(1-p)$$

for the binary entropy function, i.e., $h(p)$ is the Shannon entropy of a binary random variable that takes on one value with probability $p$ and the other with $1-p$. Note that the function $h(p)$ is *concave*, which implies that for any $0 \leq p \leq 1$ and $0 \leq c \leq 1$, we have

$$h(c \cdot p) \geq c \cdot h(p) . \tag{1}$$

We will need the chain-rule

$$H(XY|Z) = H(X|Z) + H(Y|XZ) , \tag{2}$$

and the following monotonicity inequalities

$$H(XY|Z) \geq H(X|Z) \geq H(X|YZ) , \tag{3}$$

$$I(WX;Y|Z) \geq I(X;Y|Z) . \tag{4}$$

We will also need

$$H(X|YZ) = \sum_z P_Z(z) \cdot H(X|Y, Z = z) . \tag{5}$$

$X \leftrightarrow Y \leftrightarrow Z$ implies that

$$H(X|Z) \geq H(X|YZ) = H(X|Y) . \tag{6}$$

It is easy to show that if $W \leftrightarrow XZ \leftrightarrow Y$, then

$$I(X;Y|ZW) \leq I(X;Y|Z) \text{ and} \tag{7}$$

$$I(W;Y|Z) \leq I(X;Y|Z) . \tag{8}$$

We will need the following lemma that we prove in Appendix C.

*Lemma 1:* Let $(X,Y)$, and $(\hat{X}, \hat{Y})$ be random variables distributed according to $P_{XY}$ and $P_{\hat{X}\hat{Y}}$, and let $\mathrm{D}(P_{XY}, P_{\hat{X}\hat{Y}}) \leq \epsilon$. Then

$$H(\hat{X}|\hat{Y}) \geq H(X|Y) - \epsilon \log |\mathcal{X}| - \mathrm{h}(\epsilon) .$$

Lemma 1 implies Fano's inequality: For all $X, \hat{X} \in \mathcal{X}$ with $\Pr[X \neq \hat{X}] \leq \varepsilon$, we have

$$H(X|\hat{X}) \leq \varepsilon \cdot \log |\mathcal{X}| + h(\varepsilon) . \tag{9}$$

### B. Smooth Entropies

The *min-entropy* $H_{\min}(X)$ is the negative logarithm of the probability of the most likely element

$$H_{\min}(X) := - \log \max_x P_X(x) .$$

The *max-entropy* is defined as the logarithm of the size of the support of $P_X$

$$H_{\max}(X) := \log |\text{supp}\,(P_X)| .$$

There is no standard definition of conditional min- or max-entropy. A natural definition of the min-entropy[3] is the following

$$\begin{aligned} H_{\min}(X|Y) : &= - \log \sum_y P_Y(y) \max_x P_{X|Y=y}(x) \\ &= - \log \sum_y \max_x P_{XY}(x,y) . \end{aligned}$$

Then $2^{-H_{\min}(X|Y)}$ corresponds to the maximal probability to guess $X$ from $Y$. In contrast to Shannon entropy, min- and max-entropies are not robust to small changes in the distribution. Therefore, one often considers smoothed versions of these measures, where the entropy is optimized over a set of distributions that are close in terms of some distance measure. While the concept of smoothed entropies has already been used in the literature on randomness extraction [45], the term *smooth entropy* has been introduced in [46]. There it has been shown that the smoothed conditional min- and max-entropy[4] have similar properties as the Shannon entropy, i.e., they satisfy a chain rule, monotonicity and subadditivity.

[2] All logarithms are binary.

[3] This definition has been introduced in [43] in the context of cryptography. Furthermore, it corresponds to the definition of quantum conditional min-entropy [44] for the special case of classical states.

[4] The variant of conditional min-entropy used there is different from the one we consider in this article.

*Definition 1:* For random variables $X, Y$ and $\varepsilon \in [0,1)$, we define

$$H^{\varepsilon}_{\max}(X|Y) := \min_{\Omega:\Pr[\Omega]\geq 1-\varepsilon} \max_{y} \log |\mathrm{supp}\,(P_{X\Omega|Y=y})|$$
$$H^{\varepsilon}_{\min}(X|Y) := \max_{\Omega:\Pr[\Omega]\geq 1-\varepsilon} -\log \sum_{y} P_Y(y) \max_{x} P_{X\Omega|Y=y}(x) \ .$$

In Appendix B we prove various properties of the entropies $H^{\varepsilon}_{\min}(X|Y)$ and $H^{\varepsilon}_{\max}(X|Y)$.

### C. Primitives and Randomized Primitives

In the following we consider two-party primitives that take inputs $x$ from Alice and $y$ from Bob and output $\bar{x}$ to Alice and $\bar{y}$ to Bob, where $(\bar{x}, \bar{y})$ are distributed according to $P_{\bar{X}\bar{Y}|XY}$. For simplicity, we identify such a primitive with $P_{\bar{X}\bar{Y}|XY}$. If the primitive has no input and outputs values $(u, v)$ distributed according to $P_{UV}$, we may simply write $P_{UV}$. If the primitive is deterministic and only Bob gets an output, i.e., if there exists a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ such that $P_{\bar{X}\bar{Y}|X=x,Y=y}(\perp, f(x,y)) = 1$ for all $x, y$, then we identify the primitive with the function $f$.

Examples of such primitives are $\binom{n}{t}$-$\mathsf{OT}^k$, $(p)$-$\mathsf{RabinOT}^k$, $\mathsf{EQ}_n$ and $\mathsf{IP}_n$:

- $\binom{n}{t}$-$\mathsf{OT}^k$ is the primitive where Alice has an input $x = (x_0, \dots, x_{n-1}) \in \{0,1\}^{k \cdot n}$, and Bob has an input $c \subseteq \{0, \dots, n-1\}$ with $|c| = t$. Bob receives $y = x|_c \in \{0,1\}^{tk}$.
- $(p)$-$\mathsf{RabinOT}^k$ is the primitive where Alice has an input $x \in \{0,1\}^k$. Bob receives $y$ which is equal to $x$ with probability $p$ and $\Delta$ otherwise.
- The *equality* function $\mathsf{EQ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined as
$$\mathsf{EQ}_n(x,y) := \begin{cases} 1, & \text{if } x = y \ , \\ 0, & \text{otherwise} \ . \end{cases}$$
- The *inner-product-modulo-two* function $\mathsf{IP}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is defined as $\mathsf{IP}_n(x,y) := \oplus_{i=1}^n x_i y_i$.

We often allow a protocol to use a primitive $P_{UV}$ that does not have any input and outputs $u$ and $v$ distributed according to the distribution $P_{UV}$ to the players. This is enough to model reductions to $\binom{n}{t}$-$\mathsf{OT}^k$ and $(p)$-$\mathsf{RabinOT}^k$, since these primitives are equivalent to distributed randomness $P_{UV}$, i.e., there exist two protocols that are secure in the semi-honest model: one that generates the distributed randomness using *one* instance of the primitive, and one that implements *one* instance of the primitive using the distributed randomness as input to the two parties. The fact that $\binom{2}{1}$-$\mathsf{OT}^1$ is equivalent to distributed randomness has been presented in [24], [47]. The generalization to $\binom{n}{t}$-$\mathsf{OT}^k$ is straightforward. The randomized primitives are obtained by simply choosing all inputs uniformly at random. For $(p)$-$\mathsf{RabinOT}^k$, the implementation is straightforward. Hence, any protocol that uses some instances of $\binom{n}{t}$-$\mathsf{OT}^k$ or $(p)$-$\mathsf{RabinOT}^k$ can be converted into a protocol that only uses a primitive $P_{UV}$ without any input.

### D. Protocols and Security in the Semi-Honest Model

We will consider the following model: The two parties use a primitive $P_{UV}$ that has no input and outputs values $(u, v)$ distributed according to $P_{UV}$ to the players. Alice and Bob receive inputs $x$ and $y$. Then, the players exchange messages in several rounds, where we assume that Alice sends the first message. If $i$ is odd, then Alice computes the $i$-th message as a randomized function of all previous messages, her input $x$ and $u$. If $i$ is even, then Bob computes the $i$-th message as a randomized function of all previous messages, his input $y$ and $v$. We assume that the number of rounds is bounded by a constant $t$. By padding the protocol with empty rounds, we can thus assume without loss of generality that the protocol uses $t$ rounds in every execution. After $t$ rounds, Bob computes his output $\tilde{z}$ as a randomized function of $(M, V, y)$, where $M = (M_1, \dots, M_t)$ is the sequence of all messages exchanged. It is easy to check that inequalities (7) and (8) imply that, for every distribution of the inputs $X$ and $Y$, we have $I(\tilde{Z}; XU|YVM) = 0$, $I(\tilde{Z}Y; X|VM) = 0$ and $I(\tilde{Z}YV; X|UM) = 0$.

We will consider the *semi-honest model*, where both players behave honestly, but may save all the information they get during the protocol to obtain extra information about the other player's input or output. A protocol securely implements $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ with an error $\varepsilon$, if the entire view of each player can be simulated with an error of at most $\varepsilon$ in an ideal setting, where the players only have black-box access to the primitive $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. Note that this simulation is allowed to change neither the input nor the output. This definition of security follows Definition 7.2.1 from [48], but is adapted to the case of computationally unbounded adversaries and statistical indistinguishability.

*Definition 2:* Let $\Pi$ be a *protocol with black-box access to a primitive* $P_{UV}$ that implements a primitive $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. The random variables $View^{\Pi}_A(x,y)$ and $View^{\Pi}_B(x,y)$ denote the views of Alice and Bob on input $(x,y)$ defined as $(x, u, m_1, \dots, m_t, r_A)$ and $(x, v, m_1, \dots, m_t, r_B)$, respectively, where $r_A$ ($r_B$) is the private randomness of Alice (Bob), $m_i$ represents the $i$-th message and $u, v$ is the output from $P_{UV}$. $Out^{\Pi}_B(x,y)$ denotes the output (which is implicit in the view) of Bob on input $(x,y)$. The protocol is secure in the semi-honest model with an error of at most $\varepsilon$, if there exist two randomized functions $S_A$ and $S_B$, called the simulators[5], such that for all $x$ and $y$:

$$\mathrm{D}((View^{\Pi}_A(x,y), Out^{\Pi}_B(x,y)), (S_A(x), z)) \leq \varepsilon \ ,$$
$$\mathrm{D}((z, S_B(y,z)), (Out^{\Pi}_B(x,y), View^{\Pi}_B(x,y))) \leq \varepsilon \ ,$$

where $z = f(x,y)$.

Note that security in the semi-honest model does not directly imply security in the malicious model, as the simulator is allowed to change the input/output in the malicious model, while he is not allowed to do so in the semi-honest model. We will, therefore, also consider security in the *weak semi-honest model*, which is implied both by security in the semi-honest model and by security in the malicious model. Here, the

[5] We do not require the simulator to be efficient.

simulator is allowed to change the input to the ideal primitive and change the output from the ideal primitive. Thus, in order to show impossibility of certain protocols in the malicious and in the semi-honest model, it is sufficient to show impossibility in the weak semi-honest model.

### E. Sufficient Statistics

Intuitively speaking, the sufficient statistics of $X$ with respect to $Y$, denoted $X \searrow Y$, is the part of $X$ that is correlated with $Y$.

*Definition 3:* Let $X$ and $Y$ be random variables, and let $f(x) = P_{Y|X=x}$. The sufficient statistics of $X$ with respect to $Y$ is defined as $X \searrow Y = f(X)$.
It is easy to show (see for example [49]) that for any $P_{XY}$, we have $X \leftrightarrow X \searrow Y \leftrightarrow Y$. This immediately implies that any protocol with access to a primitive $P_{UV}$ can be transformed into a protocol with access to $P_{U \searrow V, V \searrow U}$ (without compromising the security) because the players can compute $P_{UV}$ from $P_{U \searrow V, V \searrow U}$ privately. Thus, in the following we only consider primitives $P_{UV}$ where $U = U \searrow V$ and $V = V \searrow U$.

### F. Common Part

The common part was first introduced in [50]. In a cryptographic context, it was used in [17]. Roughly speaking, the common part $X \wedge Y$ of $X$ and $Y$ is the maximal element of the set of all random variables (i.e., the *finest* random variable) that can be generated both from $X$ and from $Y$ without any error. For example, if $X = (X_0, X_1) \in \{0,1\}^2$ and $Y = (Y_0, Y_1) \in \{0,1\}^2$, and we have $X_0 = Y_0$ and $\Pr[X_1 \neq Y_1] = \varepsilon > 0$, then the common part of $X$ and $Y$ is equivalent to $X_0$.

*Definition 4:* Let $X$ and $Y$ be random variables with distribution $P_{XY}$. Let $\mathcal{X} := \operatorname{supp}(P_X)$ and $\mathcal{Y} := \operatorname{supp}(P_Y)$. Then $X \wedge Y$, the *common part* of $X$ and $Y$, is constructed in the following way:

- Consider the bipartite graph $G$ with vertex set $\mathcal{X} \cup \mathcal{Y}$, and where two vertices $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ are connected by an edge if $P_{XY}(x, y) > 0$ holds.
- Let $f_X : \mathcal{X} \to 2^{\mathcal{X} \cup \mathcal{Y}}$ be the function that maps a vertex $v \in \mathcal{X}$ of $G$ to the set of vertices in the connected component of $G$ containing $v$. Let $f_Y : \mathcal{Y} \to 2^{\mathcal{X} \cup \mathcal{Y}}$ be the function that does the same for a vertex $w \in \mathcal{Y}$ of $G$.
- $X \wedge Y :\equiv f_X(X) \equiv f_Y(Y)$ .

## III. Impossibility Results for Classical Secure Function Evaluation

Let a protocol be an $\varepsilon$-secure implementation of a primitive $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ in the semi-honest model. Let $P_{XY}$ be the input distribution and let $M$ be the whole communication during the execution of the protocol. Then the security of the protocol implies the following lemma that we will use in our proofs.

*Lemma 2:*

$$H(X|VM) \geq H(X|Yf(X,Y)) - \varepsilon \log |\mathcal{X}| - h(\varepsilon) \ .$$

*Proof:* The security of the protocol implies that there exists a randomized function $S_B$, the simulator, such that $\mathrm{D}(P_{XYS_B(Y,f(X,Y))}, P_{XYVM}) \leq \varepsilon$. We can use Lemma 1 and (6) to obtain

$$\begin{aligned} H(X|VM) &\geq H(X|S_B(Y, f(X,Y))) - \varepsilon \log |\mathcal{X}| - h(\varepsilon) \\ &\geq H(X|Yf(X,Y)) - \varepsilon \log |\mathcal{X}| - h(\varepsilon) \ . \end{aligned}$$

■

We will now give lower bounds for information-theoretically secure implementations of functions $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ from a primitive $P_{UV}$ in the semi-honest model. Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function such that

$$\forall x \neq x' \in \mathcal{X}\ \exists y \in \mathcal{Y} :\ f(x,y) \neq f(x',y) \ . \qquad (10)$$

This means that it is possible to compute $x$ from the set $\{(f(x,y), y) \ : \ y \in \mathcal{Y}\}$ for any $x$. In any secure implementation of $f$, Alice does not learn which $y$ Bob has chosen, but has to make sure that Bob can compute $f(x,y)$ for any $y$. This implies that she cannot hold back any information about $x$. The statement of Lemma 3 formally captures this intuition.

Unless otherwise specified, we assume that Alice and Bob choose their inputs $X$ and $Y$ uniformly at random in the following.

*Lemma 3:* For any protocol that is an $\varepsilon$-secure implementation of a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ that satisfies (10) in the semi-honest model, we have for any $y \in \mathcal{Y}$

$$H(X|UM, Y = y) \leq (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon))$$

*Proof:* There exists a randomized function $S_A$, the simulator, such that

$$\mathrm{D}(P_{XMU|Y=y}, P_{XS_A(X)}) \leq \varepsilon$$

for all $y \in \mathcal{Y}$. Therefore, the triangle inequality implies that for any $y, y'$

$$\mathrm{D}(P_{XMU|Y=y}, P_{XMU|Y=y'}) \leq 2\varepsilon \ . \qquad (11)$$

It holds that $I(X; Z|UM, Y = y) = 0$. Furthermore, we have $\Pr[Z \neq f(X,Y) \mid Y = y] \leq \varepsilon$. Thus, it follows from (6) and (9) that

$$\begin{aligned} H(f(X,y)|UM, Y = y) &\leq H(f(X,y)|Z, Y = y) \\ &\leq \varepsilon \cdot \log |\mathcal{Z}| + h(\varepsilon) \ . \qquad (12) \end{aligned}$$

Together with (11) and Lemma 1 this implies that for any $y, y'$

$$\begin{aligned} H(f(X,y)|UM, Y = y') &\leq 3\varepsilon \log |\mathcal{Z}| + h(\varepsilon) + h(2\varepsilon) \\ &\leq 3(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) \ , \end{aligned}$$

where the second inequality follows from (1). Since $X$ can be computed from the values $f(X, y_1), \ldots, f(X, y_{|\mathcal{Y}|})$, we obtain

$$\begin{aligned} &H(X|UM, Y = y) \\ &\quad \leq H(f(X,y_1), \ldots f(X, y_{|\mathcal{Y}|})|UM, Y = y) \\ &\quad \leq \sum_{y' \in \mathcal{Y}} H(f(X,y')|UM, Y = y) \\ &\quad \leq (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) \ , \end{aligned}$$

where we used (3) in the first and (2) and (3) in the second inequality. ■

*Theorem 1:* Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function that satisfies (10). If there exists a protocol that implements $f$ from a primitive $P_{UV}$ with an error $\varepsilon$ in the semi-honest model, then

$$\begin{aligned} H(U|V) \geq \max_y & H(X|f(X,y)) \\ & - (3|\mathcal{Y}| - 1)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) - \varepsilon \log |\mathcal{X}| \ . \end{aligned}$$

*Proof:* Let $y \in \mathcal{Y}$. By Lemma 3 and inequality (3), we conclude that

$$\begin{aligned} H(X|UVM, Y = y) &\leq H(X|UM, Y = y) \\ &\leq (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) \ . \end{aligned}$$

We can use (3), (2) and Lemma 1 to obtain

$$\begin{aligned} & H(X|VM, Y = y) \\ & \quad = H(U|VM, Y = y) + H(X|UVM, Y = y) \\ & \qquad - H(U|XVM, Y = y) \\ & \quad \leq H(U|VM, Y = y) + (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) \\ & \quad \leq H(U|V) + (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon)) \ . \end{aligned}$$

By Lemma 2, we know that

$$H(X|f(X,y)) - \varepsilon \log |\mathcal{X}| - h(\varepsilon) \leq H(X|VM, Y = y) \ .$$

The statement follows by maximizing over all $y$. ■

Note that in (12) the term $\log |\mathcal{Z}|$ could be replaced by

$$d_f := \log \max_y |\{f(x,y) : \ x \in \mathcal{X}\}| \leq \log \min(|\mathcal{Z}|, |\mathcal{X}|).$$

The resulting bound,

$$\begin{aligned} H(U|V) \geq \max_y & H(X|f(X,y)) \\ & - (3|\mathcal{Y}| - 1)(\varepsilon \cdot d_f + h(\varepsilon)) - \varepsilon \log |\mathcal{X}| \ , \end{aligned}$$

is stronger in general, but does not lead to improved results for the examples considered here.

If the domain $|\mathcal{Y}|$ of a function is large, Theorem 1 may only imply a rather weak bound. A simple way to improve this bound is to restrict the domain of $f$, i.e., to consider a function $f'(x,y) : \mathcal{X}' \times \mathcal{Y}' \to \mathcal{Z}$ where $\mathcal{X}' \subset \mathcal{X}$ and $\mathcal{Y}' \subset \mathcal{Y}$ with $f'(x,y) = f(x,y)$ that still satisfies condition (10). Clearly, if $f$ can be computed from a primitive $P_{UV}$ with an error $\varepsilon$ in the semi-honest model, then $f'$ can be computed with the same error. Thus, any lower bound for $f'$ implies a lower bound for $f$.

*Corollary 3:* For any implementation of $m$ independent instances of $\binom{n}{t}$-$\mathsf{OT}^k$ from a primitive $P_{UV}$ that is $\varepsilon$-secure in the semi-honest model, the following lower bound must hold:

$$H(U|V) \geq ((1 - \varepsilon)n - t)km - (3\lceil n/t \rceil - 1)\,(\varepsilon mtk + h(\varepsilon)) \ .$$

*Proof:* We can choose subsets $C_i \subseteq \{0, \ldots, n - 1\}$, with $1 \leq i \leq \lceil n/t \rceil$, of size $t$ such that $\bigcup_{i=1}^{\lceil n/t \rceil} C_i = \{1, \ldots, n\}$, and restrict Bob to choose one of these sets as input for every instance of OT. It is easy to check that condition (10) is satisfied. The statement follows from Theorem 1. ■

For our next lower-bound, the function $f$ must satisfy the following property. Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function such that there exist $y_1 \in \mathcal{Y}$ such that

$$\forall x \neq x' \in \mathcal{X} : f(x, y_1) \neq f(x', y_1) \ , \tag{13}$$

and $y_2 \in \mathcal{Y}$ such that

$$\forall x, x' \in \mathcal{X} : f(x, y_2) = f(x', y_2) \ . \tag{14}$$

Therefore, Bob will receive Alice's whole input if his input is $y_1$, and will get no information about Alice's input if his input is $y_2$. This property can for example be satisfied by restricting Alice's input in $\binom{n}{t}$-$\mathsf{OT}^k$, as we will see in Corollary 4.

Let Alice's input $X$ be uniformly distributed. Loosely speaking, the security of the protocol implies that the communication gives (almost) no information about Alice's input $X$ if Bob's input is $y_2$. But the communication must be (almost) independent of Bob's input, otherwise Alice could learn Bob's input. Thus, Alice's input $X$ is uniform with respect to the whole communication even when Bob's input is $y_1$. Let now Bob's input be fixed to $y_1$ and let $M$ be the whole communication. The following lower bound can be proved using the given intuition.

*Lemma 4:*

$$\begin{aligned} & H(f(X, y_1)|M, U \wedge V, Y = y_1) \\ & \qquad \geq \log |\mathcal{X}| - 6(\varepsilon \log |\mathcal{X}| + h(\varepsilon)) \ . \end{aligned}$$

*Proof:* Let $g_U, g_V$ be the functions that compute the common part of $P_{UV}$. As in inequality (11) in the proof of Lemma 3, we obtain that

$$\mathrm{D}(P_{XMU|Y=y}, P_{XMU|Y=y'}) \leq 2\varepsilon \ ,$$

for all $y \neq y' \in \mathcal{Y}$. This implies that

$$\mathrm{D}(P_{XMg_U(U)|Y=y}, P_{XMg_U(U)|Y=y'}) \leq 2\varepsilon \ , \tag{15}$$

and

$$\mathrm{D}(P_X P_{Mg_U(U)|Y=y}, P_X P_{Mg_U(U)|Y=y'}) \leq 2\varepsilon \ . \tag{16}$$

Since the protocol is secure, there exists a simulator $S_B$ such that

$$\mathrm{D}(P_{XMV|Y=y_2}, P_{XS_B(y_2, f(X,y_2))}) \leq \varepsilon \ .$$

From the property (14), we can conclude that

$$\mathrm{D}(P_{XMV|Y=y_2}, P_X P_{S_B(y_2, f(X,y_2))}) \leq \varepsilon.$$

Therefore, we can use the triangle inequality to derive the following upper bound on the distance from uniform of $X$ with respect to $Mg_U(U)$ conditioned on $y_2$:

$$\begin{aligned} & \mathrm{D}(P_{XMg_U(U)|Y=y_2}, P_X P_{Mg_U(U)|Y=y_2}) \\ & \qquad \leq \mathrm{D}(P_{XMV|Y=y_2}, P_X P_{MV|Y=y_2}) \\ & \qquad \leq \mathrm{D}(P_{XMV|Y=y_2}, P_X P_{S_B(y_2, f(X,y_2))}) \\ & \qquad \quad + \mathrm{D}(P_X P_{S_B(y_2, f(X,y_2))}, P_X P_{MV|Y=y_2}) \\ & \qquad \leq 2\varepsilon \ . \end{aligned} \tag{17}$$

This implies that a weaker upper bound also holds conditioned on $y_1$ as follows: We can use the triangle inequality again to conclude from (15), (16) and (17) that

$$\begin{aligned}\mathrm{D}(&P_{XM_{g_U(U)}|Y=y_1}, P_X P_{M_{g_U(U)}|Y=y_1})\\ &\leq \mathrm{D}(P_{XM_{g_U(U)}|Y=y_1}, P_{XM_{g_U(U)}|Y=y_2})\\ &\quad + \mathrm{D}(P_{XM_{g_U(U)}|Y=y_2}, P_X P_{M_{g_U(U)}|Y=y_2})\\ &\quad + \mathrm{D}(P_X P_{M_{g_U(U)}|Y=y_2}, P_X P_{M_{g_U(U)}|Y=y_1})\\ &\leq\ 6\varepsilon\ .\end{aligned}$$

Therefore, we obtain

$$\begin{aligned}H(f(X,y_1)|M,U\wedge V,&Y=y_1)\\ &= H(X|M,U\wedge V,Y=y_1)\\ &\geq \log|\mathcal{X}| - 6(\varepsilon\log|\mathcal{X}| - h(\varepsilon))\ ,\end{aligned}$$

where we used Lemma 1. ■

We use Lemma 4 to prove the following lower bound on the mutual information of the distributed randomness for implementations of a two-party function $f$ from a primitive $P_{UV}$ in the semi-honest model.

*Theorem 2:* Let $f : \mathcal{X}\times\mathcal{Y}\to\mathcal{Z}$ be a function that satisfies (13) and (14). Then, for any protocol that implements $f$ with an error of at most $\varepsilon$ in the semi-honest model from a primitive $P_{UV}$, the following lower bound must hold:

$$\begin{aligned}I(U;V) &\geq I(U;V|U\wedge V)\\ &\geq \log|\mathcal{X}| - 7(\varepsilon\log|\mathcal{X}| + h(\varepsilon))\ .\end{aligned}$$

*Proof:* Let Alice's input $X$ be uniformly distributed and Bob's input be fixed to $y_1$. Let $Z$ be Bob's output and $M$ the whole communication. Then Lemma 4 implies that

$$H(f(X,y_1)|M,U\wedge V) \geq \log|\mathcal{X}| - 6(\varepsilon\log|\mathcal{X}| - h(\varepsilon))\ . \tag{18}$$

Since $\Pr[Z\neq f(X,y_1)]\leq\varepsilon$ and $X\leftrightarrow VM\leftrightarrow Z$, it follows from (6) and (9) that

$$H(f(X,y_1)|VM) \leq H(f(X,y_1)|Z) \leq \varepsilon\log|\mathcal{X}| + h(\varepsilon)\ . \tag{19}$$

(18) and (19) imply, using $X\leftrightarrow UM\leftrightarrow ZYV$, (8) and (4), that

$$\begin{aligned}I(U;V|M,U\wedge V) &\geq I(X;V|M,U\wedge V)\\ &\geq I(f(X,y_1);V|M,U\wedge V)\\ &= H(f(X,y_1)|M,U\wedge V)\\ &\quad - H(f(X,y_1)|VM,U\wedge V)\\ &\geq \log|\mathcal{X}| - 7(\varepsilon\log|\mathcal{X}| - h(\varepsilon))\ .\end{aligned}$$

Let $M^i := (M_1,\ldots,M_i)$, i.e., the sequence of all messages sent until the $i$-th round. Without loss of generality, let us assume that Alice sends the message of the $(i+1)$-th round. Since, we have $M^{i+1}\leftrightarrow M^iU\leftrightarrow V$, it follows from (7) that

$$I(U;V|M^{i+1},U\wedge V) \leq I(U;V|M^i,U\wedge V)\ .$$

By induction over all rounds, it holds that

$$I(U;V|M,U\wedge V) \leq I(U;V|U\wedge V)\ .$$

The statement follows. ■

The next corollary provides a lower bound on the mutual information for implementations of $\binom{n}{t}\text{-}\mathsf{OT}^k$ from a primitive $P_{UV}$. It follows immediately from Theorem 2.

*Corollary 4:* If there exists a protocol that implements $m$ independent instances of $\binom{n}{t}\text{-}\mathsf{OT}^k$ from a primitive $P_{UV}$ with an error of at most $\varepsilon$ in the semi-honest model, then the following lower bounds must hold: If $t\leq\lfloor n/2\rfloor$, then

$$I(U;V|U\wedge V) \geq mtk - 7(\varepsilon mtk + h(\varepsilon))\ .$$

If $t>\lfloor n/2\rfloor$, then

$$I(U;V|U\wedge V) \geq m(n-t)k - 7(\varepsilon m(n-t)k + h(\varepsilon))\ .$$

*Proof:* In the first case, consider the function that is obtained by setting the first $n-t$ inputs to a fixed value and choosing the remaining $t$ inputs from $\{0,1\}^{tk}$ for every instance of OT. In the second case, we use the fact that $\binom{2n-2t}{n-t}\text{-}\mathsf{OT}^k$ can be obtained from $\binom{n}{t}\text{-}\mathsf{OT}^k$ by fixing $2t-n$ inputs. Thus, both bounds follow from Theorem 2. ■

An instance of $\binom{2}{1}\text{-}\mathsf{OT}^1$ can be implemented from one instance of $\binom{2}{1}\text{-}\mathsf{OT}^1$ in the opposite direction [51]. Therefore, it follows immediately from Corollary 1 that

$$H(V|U) \geq 1 - 5h(\varepsilon) - 7\varepsilon\ ,$$

since any violation of this bound would contradict the bound of Corollary 3. We will show that a generalization of this bound also holds for $m$ independent copies of $\binom{n}{1}\text{-}\mathsf{OT}^k$ for any $n\geq 2$. Note that we can assume that $k=1$. The resulting bound then also implies a bound for $k>1$ because one instance of $\binom{n}{1}\text{-}\mathsf{OT}^1$ can be implemented from one instance of $\binom{n}{1}\text{-}\mathsf{OT}^k$.

*Theorem 3:* Let a protocol having access to $P_{UV}$ be an $\varepsilon$-secure implementation of $m$ independent copies of $\binom{n}{1}\text{-}\mathsf{OT}^1$ in the semi-honest model. Then

$$H(V|U) \geq m\log n - m(4\log n + 7)(\varepsilon + h(\varepsilon))\ .$$

*Proof:* Let Alice and Bob choose their inputs $X = (X^1,\ldots,X^m)\in\{0,1\}^{mn}$, where $X^i = (X^i_0,\ldots,X^i_{n-1})$, and $C=(C^1,\ldots,C^m)\in\{0,\ldots,n-1\}^m$ uniformly at random. Let $Y=(Y^1,\ldots,Y^m)$ be the output of Bob at the end of the protocol. Let $j\in\{1,\ldots,m\}$. First, we consider the $j$th instance of $\binom{n}{1}\text{-}\mathsf{OT}^1$. Let $A_i := X^j_0\oplus X^j_i$, for $i\in\{1,\ldots,n-1\}$. From the security of the protocol follows that there exists a randomized function $S_B(c,x_c)$ such that for all $a=(a_1,\ldots,a_{n-1})\in\{0,1\}^{n-1}$,

$$\mathrm{D}(P_{YCVM|A=a}, P_{X_C C S_B(C,X_C)}) \leq \varepsilon\ .$$

Hence, the triangle inequality implies that

$$\begin{aligned}\mathrm{D}(P_{Y^jC^jVM|A=a},&P_{Y^jC^jVM|A=a'})\\ &\leq \mathrm{D}(P_{YCVM|A=a}, P_{YCVM|A=a'})\\ &\leq 2\varepsilon\end{aligned} \tag{20}$$

holds for all $a,a'$. We have $\Pr[Y^j\neq X^j_C \mid A=a]\leq\varepsilon$ for all $a$. If $A=(0,\ldots,0)$, we have $X^j_C = X^j_0$. Since $X^j\leftrightarrow$

$VM \leftrightarrow Y^j$, it follows from (3) and (9) that

$$\begin{aligned} H(Y^j|VM, A=(0,\dots,0)) &\le H(Y^j|X^j, A=(0,\dots,0)) \\ &\le H(Y^j|X_0^j, A=(0,\dots,0)) \\ &\le \varepsilon + h(\varepsilon) \ . \end{aligned} \tag{21}$$

Now, we map $C^j$ to a bit string of size $\lceil \log n \rceil$. Let $C_b$ be the $b$-th bit of that bit string, where $b \in \{0, \dots, \lceil \log n \rceil - 1\}$. Let $a^b = (a_1^b, \dots, a_{n-1}^b)$, where $a_i^b = 1$ if and only if the $b$-th bit of $i$ is 1. Conditioned on $A = a^b$, we have $X_C^j = X_0^j \oplus C_b$. It follows from $X^j \leftrightarrow VM \leftrightarrow Y^jC^j$, (3) and (9) that

$$\begin{aligned} H(Y^j \oplus C_b|VM, A=a^b) &\le H(Y^j \oplus C_b|X_0^j, A=a^b) \\ &\le \varepsilon + h(\varepsilon) \ . \end{aligned} \tag{22}$$

By Lemma 1, (20) and (21), we obtain

$$H(Y^j|VMA) \le \varepsilon + h(\varepsilon) + 2\varepsilon + h(2\varepsilon) \le 3\varepsilon + 3h(\varepsilon).$$

It follows from Lemma 1, (20) and (22) that for all $b$

$$H(Y^j \oplus C_b|VMA) \le 3\varepsilon + 3h(\varepsilon) \ .$$

Since $(C^j, Y^j)$ can be calculated from $(Y^j, Y^j \oplus C_0, \dots, Y^j \oplus C_{\lceil \log n \rceil - 1})$, this implies that

$$H(C^jY^j|VMA) \le 3(\lceil \log n \rceil + 1)(\varepsilon + h(\varepsilon)) \ .$$

The Markov chain $A \leftrightarrow VM \leftrightarrow C^jY^j$, $\lceil \log n \rceil \le \log n + 1$ and inequality (3) imply that

$$H(C^j|VM) \le 3(\log n + 2)(\varepsilon + h(\varepsilon)) \ .$$

Thus we can use (2) and (3) to obtain

$$\begin{aligned} H(C|VM) &\le \sum_{j=1}^{n} H(C^j|VM) \\ &\le 3m(\log n + 2)(\varepsilon + h(\varepsilon)) \ . \end{aligned}$$

We can use (2), (3) and Lemmas 1 to obtain

$$\begin{aligned} H(C|UM) &= H(V|UM) + H(C|UVM) - H(V|CUM) \\ &\le H(V|UM) + 3m(\log n + 2)(\varepsilon + h(\varepsilon)) \\ &\le H(V|U) + 3m(\log n + 2)(\varepsilon + h(\varepsilon)) \ . \end{aligned}$$

The security of the protocol implies that there exists a randomized function $S_A$ such that $\mathrm{D}(P_{CS_A(X)}, P_{CUM}) \le \varepsilon$. Using Lemma 1 and inequality (6), we obtain that

$$\begin{aligned} H(C|UM) &\ge H(C|S_A(X)) - \varepsilon m \log n - h(\varepsilon) \\ &\ge H(C|X) - \varepsilon m \log n - h(\varepsilon) \end{aligned}$$

■

Altogether, Corollary 3, Corollary 4 and Theorem 3 prove the following theorem.

*Theorem 4:* If there exists a protocol having access to $P_{UV}$ that implements $m$ instances of $\binom{n}{1}$-$\mathsf{OT}^k$ with an error of at most $\varepsilon$ in the semi-honest model, then

$$\begin{aligned} H(U|V) &\ge m(n-1)k - (4n-1)(\varepsilon mk + h(\varepsilon)) \ , \\ H(V|U) &\ge m \log n - m(4 \log n + 7)(\varepsilon + h(\varepsilon)) \ , \\ I(U;V|U \wedge V) &\ge mk - 7\varepsilon mk - 7h(\varepsilon) \ . \end{aligned}$$

Since $m$ instances of $\binom{n}{1}$-$\mathsf{OT}^k$ are equivalent to a primitive $P_{UV}$ with $H(U|V) = m(n-1)k$, $I(U;V) = mk$ and $H(V|U) = m \log n$, any protocol that implements $M$ instances of $\binom{N}{1}$-$\mathsf{OT}^K$ from $m$ instances of $\binom{n}{1}$-$\mathsf{OT}^k$ with an error of at most $\varepsilon$ needs to satisfy the following inequalities:

$$\begin{aligned} m(n-1)k &\ge M(N-1)K - (4N-1)(\varepsilon MK + h(\varepsilon)) \ , \\ mk &\ge MK - 7\varepsilon MK - 7h(\varepsilon) \ , \\ m \log n &\ge M \log N - M(4 \log N + 7)(\varepsilon + h(\varepsilon)) \ . \end{aligned}$$

Thus, we get Corollary 1.

We will now use the proof of Theorem 1 and the smooth entropy formalism to derive a lower bound on the conditional min-entropy for information-theoretically secure implementations of functions $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ from a primitive $P_{UV}$ in the semi-honest model. As a motivation, consider the following question: is it possible to $\varepsilon$-securely implement $\binom{2}{1}$-$\mathsf{OT}^K$ from $(1/2)$-$\mathsf{RabinOT}^k$? Corollary 3 only tells us that $K$ must be smaller than or equal to $k/2$. Our lower bound on the conditional smooth min-entropy, however, implies that there is no such implementation if $K \ge 2$ and $0 \le \varepsilon < 0.25$, independently of $k$.

Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function that satisfies (10). Let Alice and Bob choose their inputs $X$ and $Y$ uniformly at random and let $M$ be the whole communication during the protocol. For the rest of this section, we assume that all parameters are sufficiently small such that the smoothing parameters of the smooth entropies are always in $[0, 1)$.

*Lemma 5:* If there exists an $\varepsilon$-secure implementation of $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ from a primitive $P_{UV}$ in the (weak) semi-honest model, then

$$H_{\max}^{3|\mathcal{Y}|\varepsilon}(X|UM, Y=y) = 0 \ .$$

*Proof:* Since the protocol is secure for Bob, there exists a randomized function $S_A$ such that

$$\mathrm{D}(P_{XMU|Y=y}, P_{XS_A(X)}) \le \varepsilon$$

for all $y \in \mathcal{Y}$. Therefore, for any $y, y'$

$$\mathrm{D}(P_{XMU|Y=y}, P_{XMU|Y=y'}) \le 2\varepsilon \ . \tag{23}$$

It holds that $I(X;Z|UM, Y=y) = 0$. Furthermore, we have $\Pr[Z \neq f(X,Y) \mid Y = y] \le \varepsilon$. Thus, Lemmas 18 and 19 imply that

$$H_{\max}^{\varepsilon}(f(X,y)|UM, Y=y) \le H_{\max}^{\varepsilon}(f(X,y)|Z, Y=y) = 0 \ . \tag{24}$$

Together with (23), this implies that for any $y, y'$

$$H_{\max}^{3\varepsilon}(f(X,y)|UM, Y=y') = 0 \ .$$

Since $X$ can be computed from the values $f(X, y_1), \dots, f(X, y_{|\mathcal{Y}|})$, we obtain

$$\begin{aligned} & H_{\max}^{3|\mathcal{Y}|\varepsilon}(X|UM, Y=y) \\ &\qquad \le H_{\max}^{3|\mathcal{Y}|\varepsilon}(f(X,y_1), \dots f(X, y_{|\mathcal{Y}|})|UM, Y=y) \\ &\qquad \le \sum_{y' \in \mathcal{Y}} H_{\max}^{3\varepsilon}(f(X,y')|UM, Y=y) \\ &\qquad = 0 \ . \end{aligned}$$

where we used Lemma 19 and the subadditivity of the max-entropy (Lemma 14). ■

Let $P_{XY}$ be the input distribution to the ideal primitive. Then the security of the protocol implies the following lemma.

*Lemma 6:* For any protocol that is an $\varepsilon$-secure implementation of $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ from a primitive $P_{UV}$ in the semi-honest model,

$$H_{\min}^{\varepsilon+\varepsilon'}(X|VM) \geq H_{\min}^{\varepsilon'}(X|Yf(X,Y)) ,$$

for any $\varepsilon' \geq 0$.

*Proof:* The security of the protocol implies that there exists a randomized function $S_B$, the simulator, such that $\mathrm{D}(P_{XYS_B(Y,f(X,Y))}, P_{XYVM}) \leq \varepsilon$. Therefore, we obtain

$$\begin{aligned} H_{\min}^{\varepsilon+\varepsilon'}(X|VM) &\geq H_{\min}^{\varepsilon'}(X|S_B(Y,f(X,Y))) \\ &\geq H_{\min}^{\varepsilon'}(X|Yf(X,Y)) , \end{aligned}$$

where we used Lemma 17 in the second inequality. ■

*Theorem 5:* Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function that satisfies (10). If there exists a protocol having access to a primitive $P_{UV}$ that implements $f$ with an error of at most $\varepsilon$ in the semi-honest model, then

$$H_{\min}^{(3|\mathcal{Y}|+1)\varepsilon+\varepsilon'}(U|V) \geq \max_y H_{\min}^{\varepsilon'}(X|f(X,y)) ,$$

for any $\varepsilon' \geq 0$.

*Proof:* Let $y \in \mathcal{Y}$. It follows from Lemmas 5 and 15 that

$$H_{\max}^{3|\mathcal{Y}|\varepsilon}(X|UVM, Y=y) \leq H_{\max}^{3|\mathcal{Y}|\varepsilon}(X|UM, Y=y) = 0 .$$

Therefore, Lemma 15 and 16 implies that

$$\begin{aligned} H_{\min}^{\varepsilon+\varepsilon'}(X|VM, Y=y) - H_{\max}^{3|\mathcal{Y}|\varepsilon}(X|UVM, Y=y) \\ \leq H_{\min}^{(3|\mathcal{Y}|+1)\varepsilon+\varepsilon'}(U|VM, Y=y) \\ \leq H_{\min}^{(3|\mathcal{Y}|+1)\varepsilon+\varepsilon'}(U|V) . \end{aligned}$$

We can use Lemma 6 to obtain

$$H_{\min}^{\varepsilon'}(X|f(X,y)) \leq H_{\min}^{\varepsilon+\varepsilon'}(X|VM, Y=y) .$$

The statement follows by maximizing over all $y$. ■

### *A. Lower Bounds for Protocols implementing OT*

*Corollary 5:* Any protocol that implements $M$ instances of $\binom{N}{1}$-OT$^K$ from $m$ instances of $\binom{n}{1}$-OT$^k$ with an error of at most $0 \leq \varepsilon < \frac{1}{2(3n+1)}$ in the semi-honest model must satisfy

$$m(n-1)k \geq M(N-1)K - (6n+2)\varepsilon .$$

*Proof:* From Theorem 5 follows that

$$H_{\min}^{(3n+1)\varepsilon}(U|V) \geq M(N-1)K . \tag{25}$$

For the distribution $P_{UV}$ of randomized OTs, the entropy $H_{\min}^{\bar{\varepsilon}}(U|V)$ with $0 \leq \bar{\varepsilon} < 1$ is maximized by the event $\Omega$ with $P_{\Omega|U=u,V=v} = 1 - \bar{\varepsilon}$ for all $u, v$ in the support of $P_{UV}$. Therefore, we have

$$\begin{aligned} H_{\min}^{(3n+1)\varepsilon}(U|V) &\leq -\log(2^{-m(n-1)k}(1-(3n+1)\varepsilon)) \\ &= m(n-1)k - \log(1-(3n+1)\varepsilon) . \end{aligned} \tag{26}$$

The statement follows from the fact that $\log(1/\varepsilon) \leq 2(1-\varepsilon)$ for $1/2 \leq \varepsilon \leq 1$. ■

This corollary implies that there is no protocol that extends $\binom{2}{1}$-OT$^1$ in the semi-honest model.

*Corollary 6:* Any protocol that implements $m+1$ instances of $\binom{2}{1}$-OT$^1$ in the semi-honest model using $m$ instances of $\binom{2}{1}$-OT$^1$ must have an error $\varepsilon \geq 1/14$.

### *B. Lower Bounds for Equality Function*

*Corollary 7:* Let a protocol having access to a $P_{UV}$ be an $\varepsilon$-secure implementation of $\mathsf{EQ}_n$ in the semi-honest model. Then

$$H(U|V) \geq (1-\varepsilon)k - (3 \cdot 2^k - 1)(\varepsilon + h(\varepsilon)) - 1 ,$$

and

$$H_{\min}^{(3 \cdot 2^k+1)\varepsilon}(U|V) \geq k - 1 ,$$

for all $0 < k \leq n$. If $0 \leq \varepsilon \leq 1/(6 \cdot 2^k + 2)$ and $P_{UV}$ is equivalent to $m$ instances of $\binom{2}{1}$-OT$^1$, then

$$m \geq k - 1 - (6 \cdot 2^k + 2)\varepsilon ,$$

for all $0 < k \leq n$.

*Proof:* We can restrict the input domains of both players to the same subsets of size $2^k$. Condition (10) will still be satisfied. Thus, the corollary follows immediately from Theorems 1 and 5. ■

There exists a secure reduction of $\mathsf{EQ}_n$ to $\mathsf{EQ}_k$ ([34]): Alice and Bob compare $k$ inner products of their inputs with random strings using $\mathsf{EQ}_k$. This protocol is secure in the semi-honest model with an error of at most $2^{-k}$. Since there exists a circuit to implement $\mathsf{EQ}_k$ with $k$ XOR and $k$ AND gates, it follows from [3] that $\mathsf{EQ}_k$ can be securely implemented using $k$ instances of $\binom{4}{1}$-OT$^1$ or $3k$ instances of $\binom{2}{1}$-OT$^1$ in the semi-honest model. Since $m$ instances of $\binom{2}{1}$-OT$^1$ are equivalent to a primitive $P_{UV}$ with $H(U|V) = m$, the bound of Corollary 7 is optimal up to a factor of 3. We can improve the above construction with the following protocol that computes additive shares of $(x_1 \oplus y_1) \wedge (x_2 \oplus y_2)$ using two instances of $\binom{2}{1}$-OT$^1$: Alice chooses two random bits $r_1, r_2$ and inputs $r_1, r_1 \oplus x_1$ to the first and $r_2, r_2 \oplus x_2$ to the second instance. Bob uses $y_2$ as the choice bit for the first and $y_1$ as the choice bit for the second instance of OT. Bob receives two outputs $z_1 = r_1 \oplus x_1 y_2$ and $z_2 = r_2 \oplus x_2 y_1$. Setting $a = r_1 \oplus r_2 \oplus x_1 x_2$ and $b = z_1 \oplus z_2 \oplus y_1 y_2$, we have $a \oplus b = x_1 x_2 \oplus y_1 y_2 \oplus x_1 y_2 \oplus x_2 y_1 = (x_1 \oplus y_1) \wedge (x_2 \oplus y_2)$. Thus, we can compute $\mathsf{EQ}_k$ with $2(k-1)$ instances of $\binom{2}{1}$-OT$^1$.

### *C. Lower Bounds for Inner Product Function*

*Corollary 8:* Let a protocol having access to a primitive $P_{UV}$ be an $\varepsilon$-secure implementation of the inner product function $\mathsf{IP}_n$ in the semi-honest model. Then it holds that

$$H(U|V) \geq n - 1 - 4n(\varepsilon + h(\varepsilon))$$

and

$$H_{\min}^{(3k+1)\varepsilon}(U|V) \geq n - 1 .$$

If $P_{UV}$ is equivalent to $m$ instances of $\binom{2}{1}\text{-}\mathsf{OT}^1$ and $0 \leq \varepsilon < 1/(6n+2)$, then

$$m \geq n - 1 - (6n+2)\varepsilon \; .$$

*Proof:* Let $e_i \in \{0,1\}^n$ be the string that has a one at the $i$-th position and is zero otherwise. Let $\mathcal{S} := \{e_i : \; 1 \leq i \leq n\}$. Then the protocol is an $\varepsilon$-secure implementation of the restriction of the inner-product function to inputs from $\{0,1\}^n \times \mathcal{S}$. Since this restricted function satisfies condition (10), the statement follows from Theorem 1. ■

If $\varepsilon \leq 1/(8n)$, then it immediately follows from Corollary 8 that we need at least $n-2$ calls to $\binom{2}{1}\text{-}\mathsf{OT}^1$ to compute $\mathsf{IP}_n$ with an error of at most $\varepsilon$. Consider the following protocol from [34] that is adapted to $\binom{2}{1}\text{-}\mathsf{OT}^1$: Alice chooses $r = (r_1, \ldots, r_{n-1})$ uniformly at random and sets $r_n := \oplus_{i=1}^{n-1} r_i$. Then, for each $i$, Alice inputs $a_{i,0} := r_i$ and $a_{i,1} := x_i \oplus r_i$ to the OT and Bob inputs $y_i$. Bob receives $z_i$ from the OTs and outputs $\oplus_{i=1}^n z_i$. Since $\oplus_{i=1}^n z_i = \oplus_{i=1}^n (x_i y_i \oplus r_i) = (\oplus_{i=1}^n x_i y_i) \oplus (\oplus_{i=1}^n r_i) = \oplus_{i=1}^n x_i y_i = \mathsf{IP}_n(x,y)$, the protocol is correct. The security for Alice follows from the fact that $z_1, \ldots, z_n$ is a uniformly random string subject to $\oplus_{i=1}^n z_i = \mathsf{IP}_n(x,y)$. Thus, there exists a perfectly secure protocol that computes $\mathsf{IP}_n$ from $n$ instances of $\binom{2}{1}\text{-}\mathsf{OT}^1$. Hence, Corollary 8 is almost tight.

### *D. Lower Bounds for Protocols implementing OLFE*

We will now show that Theorems 1 and 2 also imply bounds for *oblivious linear function evaluation* ($(q)$-$\mathsf{OLFE}$), which is defined as follows:

- For any finite field $GF(q)$ of size $q$, $(q)$-$\mathsf{OLFE}$ is the primitive where Alice has an input $a, b \in GF(q)$ and Bob has an input $c \in GF(q)$. Bob receives $d = a + b \cdot c \in GF(q)$.

*Corollary 9:* Let a protocol having access to $P_{UV}$ be an $\varepsilon$-secure implementation of $m$ instances of $(q)$-$\mathsf{OLFE}$ in the semi-honest model. Then

$$\begin{aligned} H(U|V) &\geq m \log q - 5(\varepsilon m \log q + h(\varepsilon)) \; , && (27)\\ H(V|U) &\geq m \log q - 5(\varepsilon m \log q + h(\varepsilon)) \; , && (28)\\ I(U;V|U \wedge V) &\geq m \log q - 7(\varepsilon m \log q + h(\varepsilon)) \; . && (29) \end{aligned}$$

*Proof:* Inequalities (27) and (29) follow from Theorem 1 and Theorem 2. Furthermore, it has been shown in [51] that $(q)$-$\mathsf{OLFE}$ is symmetric. Hence, a violation of (28) would imply a violation of the lower bound in (27). ■

### *E. Lower Bounds for OT in the Malicious Model*

In Appendix A, we show that lower bounds in the semi-honest model imply almost the same bounds in the malicious model. In the following, we generalize these results by allowing a dishonest Bob to additionally receive randomness $V'$. Moreover, the following provides a stronger impossibility result, in the case when $V'$ is trivial, than the one that follows from the combination of Lemma A.1 and Theorem 5.

*Corollary 10:* Let a protocol be an $\varepsilon$-secure implementation of $\binom{2}{1}\text{-}\mathsf{OT}^n$ in the malicious model from randomness $(U, VV')$. Then

$$H_{\min}^{7\varepsilon}(U|VV') \geq k \; .$$

*Proof:* We consider only honest players, but allow the simulator to change the inputs to the ideal OT and the outputs from the ideal OT. Lemma 5 holds in the weak semi-honest model and, therefore, also in the malicious model. Thus, we have $H_{\max}^{6\varepsilon}(X|UM, C=c) = 0$ , where $C$ is the choice bit of Bob. The security of the protocol implies that there exists a randomized function $S_B$ such that

$$\mathrm{D}(P_{XS_B(C,X_{\tilde{C}})}, P_{XVV'M}) \leq \varepsilon, \qquad (30)$$

where $\tilde{C}$ is the input to the ideal OT by the simulator. Therefore, we get

$$\begin{aligned} H_{\min}^{\varepsilon}(X|VV'M, C=c) &\geq H_{\min}(X|S_B(c, X_{\tilde{C}}))\\ &\geq H_{\min}(X|X_{\tilde{C}})\\ &\geq k \; . \end{aligned}$$

As in the proof of Theorem 5, this implies

$$k \leq H_{\min}^{\varepsilon}(X|VV'M, C=c) \leq H_{\min}^{7\varepsilon}(U|VV') \; .$$

■

In the same way, we can show that the impossibility result for implementations of $\binom{2}{1}\text{-}\mathsf{OT}^k$ that follows from Theorem 1 also holds in the malicious model.

*Corollary 11:* Let a protocol be an $\varepsilon$-secure implementation of $\binom{2}{1}\text{-}\mathsf{OT}^k$ in the malicious model from randomness $(U, VV')$. Then

$$H(U|VV') \geq k - 6(k\varepsilon + h(\varepsilon)) \; .$$

*Proof:* Since Lemma 3 also holds in the malicious model, inequality (3) implies that

$$\begin{aligned} H(X|UVV'M, C=c) &\leq H(X|UM, C=c)\\ &\leq 4(k\varepsilon + h(\varepsilon)) \; . \end{aligned}$$

We can use inequalities (1) and (30) to obtain

$$\begin{aligned} H(X|VV'M, C=c) &\geq H(X|S_B(c, X_{\tilde{C}})) - \varepsilon \cdot 2k - h(\varepsilon)\\ &\geq H(X|X_{\tilde{C}}) - \varepsilon \cdot 2k - h(\varepsilon)\\ &\geq k - \varepsilon \cdot 2k - h(\varepsilon) \; . \end{aligned}$$

As in the proof of Theorem 1, this implies

$$H(U|VV') \geq k - 6(k\varepsilon + h(\varepsilon)).$$

■

Corollary 10 can be applied to implementations of $\binom{2}{1}\text{-}\mathsf{OT}^k$ from Universal OT over bits. Universal OT [21] is a weakened variant of Bit-OT where a dishonest Bob can choose a channel $P_{Y|X}$ such that $H(X_0X_1|Y) \geq \alpha$, where $(X_0, X_1) \in \{0,1\} \times \{0,1\}$ are uniform and $Y$ is the output of the channel $P_{Y|X}$, and learns $Y$. One choice of a dishonest Bob is the channel that outputs both inputs with probability $1-\alpha$ and one of the inputs, $X_c$, with probability $\alpha$. This primitive can be implemented from randomness $(U, VV') = ((X_0, X_1), (C, X_C, V'))$, where $(U, V)$ corresponds to a randomized $\binom{2}{1}\text{-}\mathsf{OT}^1$ and $V' = X_{1-C}$ with probability $1-\alpha$ and

$V' = \perp$ otherwise. For this primitve we have $H(U|VV') \leq \alpha$ and, therefore, for $n$ independent instances $H(U^n|(VV')^n) \leq \alpha n$. Thus, Corollary 10 implies that $k \leq \alpha n + 6(k\varepsilon + h(\varepsilon))$. As Univeral OT is strictly weaker than this primitive, the same bound also applies to Universal OT. The protocol proposed in [35] which implements $\binom{2}{1}$-$\mathsf{OT}^k$ from $n$ instances of Universal OT asymptotically achieves a rate $k/n$ of $\alpha$ [52]. Our lower bound now shows that this is in fact optimal.

## IV. Quantum Reductions: Reversing String OT Efficiently

As the bounds of the last section generalize the known bounds for perfect implementations of OT from [28], [11], [12], [30] to the statistical case, it is natural to ask whether similar bounds also hold for quantum protocols, i.e., if the bounds presented in [53] can be generalized to the statistical case. We give a negative answer to this question by presenting a statistically secure quantum protocol that violates these bounds. Thereto we introduce the following functionality[6] $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ that can be implemented from $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$ (i.e., $\binom{n}{1}$-$\mathsf{OT}^k$) as we will show.

*Definition 5 (Multi-Commitment):* The functionality $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ behaves as follows: Upon (the first) input (commit, b) with $b \in \{0,1\}^k$ from Alice, send committed to Bob. Upon input (open,T) with $T \subseteq [k]$ from Alice send (open, $b_T$) to Bob. All communication/input/output is classical. We call Alice the sender and Bob the receiver.

An instance of $\binom{2}{1}$-$\mathsf{OT}^k$ can be implemented from $m = O(k+\kappa)$ bit commitments with an error of $2^{-\Omega(\kappa)}$ [24], [25], [26]. In the protocol, Alice sends $m$ BB84-states to Bob who measures them either in the computational or in the Hadamard basis. To ensure that he really measures Bob has to commit to the basis he has measured in and the measurement outcome for every qubit received. Alice then asks Bob to open a small subset $\mathcal{T}$ of these pairs of commitments. OT can then be implemented using further classical processing (see Section VI for a complete description of the protocol). This protocol implements oblivious transfer that is statistically secure in the quantum *universal composability* model [27]. Obviously the construction remains secure if we replace the commitment scheme with $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,2m}$.

Next, we show that $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ can be implemented from the oblivious transfer functionality $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$ (see [27] for a definition of $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$) using Protocol MCOMfromOT.

Protocol **MCOMfromOT**
Inputs: Alice has an input $b = (b_1, \ldots, b_k) \in \{0,1\}^k$ in Commit. Bob has an input $T \subseteq [k]$ in Open.
Commit($b$):
For all $1 \leq i \leq \kappa$:

1) Alice and Bob invoke $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$ with random inputs $x_0^i, x_1^i \in \{0,1\}^k$ and $c^i \in \{0,1\}$.
2) Bob receives $y^i = x_{c^i}^i$ from $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$.
3) Alice sends $m^i := x_0^i \oplus x_1^i \oplus b$ to Bob.

Open(T):

1) Alice sends $b_T$, $T$ and $(x_0^i)_T, (x_1^i)_T$ for all $1 \leq i \leq \kappa$ to Bob.
2) If $(m^i)_T = (x_0^i \oplus x_1^i \oplus b^i)_T$ and $(y^i)_T = (x_c^i)_T$ for all $1 \leq i \leq \kappa$, Bob accepts and outputs $b_T$, otherwise he rejects.

As it is done in the proofs of [27], we assume that all communication between the players is over secure channels and we only consider static adversaries.

*Lemma 7:* Protocol MCOMfromOT is statistically secure and universally composable and realizes $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ with an error of $2^{-\kappa/2}$ using $\kappa$ instances of $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$.

*Proof:* The statement is obviously true in the case of no corrupted parties and in the case when both the sender and the receiver are corrupted. We construct for any adversary $\mathcal{A}$ a simulator $\mathcal{S}$ that runs a copy of $\mathcal{A}$ as a black-box. In the case where the sender is corrupted, the simulator $\mathcal{S}$ can extract the commitment $b$ from the input to $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$ and the messages except with probability $2^{-\kappa/2}$ as follows: We define the extracted commitment as $b_i := \mathrm{maj}(m_i^1 \oplus x_{0,i}^1 \oplus x_{1,i}^1, \ldots, m_i^\kappa \oplus x_{0,i}^\kappa \oplus x_{1,i}^\kappa)$ for all $1 \leq i \leq k$ where maj denotes the majority function. Let $\mathcal{T}$ be a (non-empty) subset of $[k]$ and let $\tilde{b} \in \{0,1\}^k$ such that $\tilde{b}_\mathcal{T} \neq b_\mathcal{T}$. An honest receiver accepts $\tilde{b}_\mathcal{T}$ together with $\mathcal{T}$ in Open with probability at most $2^{-\kappa/2}$ as follows: There must exist $j \in \mathcal{T}$ such that $b_j \neq \tilde{b}_j$. Then the sender needs to change either $x_{0,j}^i$ or $x_{1,j}^i$ for at least $\kappa/2$ instances $i$. Thus, the simulator extracts the bit $b$ in the commit phase as specified before and gives $(\texttt{commit}, b)$ to $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$. Upon getting $(\tilde{b}, \mathcal{T})$ from the adversary, the simulator gives $(\texttt{open}, \mathcal{T})$ to $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$, if $\tilde{b}_\mathcal{T} = b_\mathcal{T}$, otherwise it stops. Therefore, any environment can distinguish the simulation and the real execution with an advantage of at most $2^{-\kappa/2}$. In the case where the receiver is corrupted, the simulator $\mathcal{S}$, upon getting the message committed from $\mathcal{F}_{\mathtt{MCOM}}^{A\to B,k}$ and the choice bit $c^i$, chooses the output $y^i$ from $\mathcal{F}_{\mathtt{OT}}^{A\to B,k}$ and the message $m^i$ uniformly and independently at random for all $i$. In the open phase the simulator $\mathcal{S}$ gets $(\mathcal{T}, b_\mathcal{T})$ and simulates the messages of an honest sender by setting $(x_{1-c^i}^i)_\mathcal{T} := (m^i)_\mathcal{T} \oplus (y^i)_\mathcal{T} \oplus b_\mathcal{T}$ and $(x_{c^i}^i)_\mathcal{T} := (y^i)_\mathcal{T}$ for all $i$. This simulation is perfectly indistinguishable from the real execution. ■

Any protocol that is statistically secure in the classical universal composability model [54] is also secure in the quantum universal composability model [27]. Together with the proofs from [26], [27], we, therefore, obtain the following theorem.

*Theorem 6:* There exists a protocol that implements $\binom{2}{1}$-$\mathsf{OT}^{k'}$ with an error $\varepsilon$ from $\kappa = O(\log 1/\varepsilon)$ instances of $\binom{2}{1}$-$\mathsf{OT}^k$ in the opposite direction where $k' = \Omega(k)$ if $k = \Omega(\kappa)$.

Since we can choose $k \gg \kappa$, this immediately implies that the bound of Corollary 3 does not hold for quantum protocols. Similar violations can be shown for the other two lower bounds (given in Corrollary 1). For example, statistically secure and

[6] In this section we will use the notion commonly used in the UC framework, that is slightly different from the rest of the paper.

universally composable[7] commitments can be implemented from shared randomness $P_{UV}$ that is distributed according to $(p)$-$\mathsf{RabinOT}$ at a rate of $H(U|V) = 1 - p$ [56]. Using Theorem 11, one can implement $\mathcal{F}_{\mathsf{OT}}^{B\to A,k}$ with $k \in \Omega(n(1-p))$ from $n$ copies of $P_{UV}$. Since $I(U;V) = p$, quantum protocols can also violate the bound of Corollary 4.

It has been an open question whether noiseless quantum communication can increase the commitment capacity [56]. Our example implies a positive answer to this question.

## V. Impossibility Results for Quantum Oblivious Transfer Reductions

We consider finite-dimensional Hilbert spaces $\mathcal{H}$. A quantum state $\rho$ is a positive semi-definite operator on $\mathcal{H}$ satisfying $\mathrm{tr}(\rho) = 1$. We use the notation $\rho_{AB}$ for a state on $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$ and define the marginal state $\rho_A := \mathrm{tr}_{\mathrm{B}}\, \rho_{AB}$. We use the symbol $\mathbb{1}_{\mathrm{A}}$ to denote either the identity operator on $\mathcal{H}_{\mathrm{A}}$ or the identity operator on the states on $\mathcal{H}_{\mathrm{A}}$; it should be clear from the context which one is meant. Given a finite set $\mathcal{X}$ and an orthonormal basis $\{|x\rangle \mid x \in \mathcal{X}\}$ of a Hilbert space $\mathcal{H}_{\mathcal{X}}$ we can encode a classical probability distribution $P_X$ as a quantum state $\rho_X = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x|$. We define the state corresponding to the uniform distribution on $\mathcal{X}$ as $\tau_{\mathcal{X}} := \frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}} |x\rangle\langle x|$. A state $\rho_{XB}$ on $\mathcal{H}_{\mathcal{X}} \otimes \mathcal{H}_{\mathrm{B}}$ is a classical-quantum or cq-state if it is of the form $\rho_{XB} = \sum_{x\in\mathcal{X}} p_x |x\rangle\langle x| \otimes \rho_B^x$. The *Hadamard transform* is the unitary described by the matrix $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ in the computational basis $\{|0\rangle, |1\rangle\}$. For $x, \theta \in \{0,1\}^n$, we write $H^\theta|x\rangle$ for the state $H^\theta|x\rangle = H^{\theta_1}|x_1\rangle \dots H^{\theta_n}|x_n\rangle$. We also call states of this form *BB84-states*. When speaking of the basis $\theta \in \{0,1\}^n$ we mean the basis $\{H^\theta|x\rangle \mid x \in \{0,1\}^n\}$. For a given basis $\{|x_1\rangle, \dots, |x_d\rangle\}$ we say that we *measure in basis* $\mathcal{B}$ to indicate that we perform a projective measurement given by the operators $P_k = |x_k\rangle\langle x_k|$ for all $k \in [d]$. The *trace distance* between two quantum states $\rho$ and $\tau$ is defined as

$$\mathrm{D}(\rho,\tau) := \max_{\mathcal{E}} D(\mathcal{E}(\rho), \mathcal{E}(\tau)) \ .$$

where the maximum is over all POVMs and $\mathcal{E}(\rho)$ is the probability distribution of the measurement outcomes. In particular, for any two cq-states $\rho_{XA}$ and $\sigma_{XA}$, $\mathrm{D}(\rho_{XA}, \sigma_{XA}) \leq \varepsilon$ implies that for any measurement $G$ on system $A$, we have

$$\big|\Pr[G(\rho_A) = X] - \Pr[G(\sigma_A) = X]\big| \leq \varepsilon \ . \tag{31}$$

If we choose $\sigma_{XA} := \tau_X \otimes \sigma_A$, this implies that

$$\Pr[G(\rho_A) = X] \leq \frac{1}{2} + \varepsilon \ . \tag{32}$$

The *conditional von Neumann entropy* is defined as

$$H(A|B)_\rho := H(\rho_{AB}) - H(\rho_B) \ ,$$

where $H(\rho) := \mathrm{tr}(-\rho\log(\rho))$. The Alicki-Fannes inequality [57] implies that

$$H(A|B)_\rho \geq (1 - 4\varepsilon) \cdot \log|A| - 2h(\varepsilon) \ , \tag{33}$$

for any state $\rho_{AB}$ with $\mathrm{D}(\rho_{AB}, \tau_A \otimes \rho_B) \leq \varepsilon$. Let $\rho_{XB}$ be a state that is classical on $X$. If there exists a measurement on $B$ with outcome $X'$ such that $\Pr[X' \neq X] \leq \varepsilon$, then

$$H(X|B)_\rho \leq H(X|X') \leq h(\varepsilon) + \varepsilon \cdot \log|X| \ . \tag{34}$$

Let $\rho_{ABC}$ be a tripartite state. Subadditivity and the triangle inequality [58] imply that

$$H(A|BC)_\rho \geq H(A|B)_\rho - 2H(C)_\rho \ . \tag{35}$$

The conditional entropy $H(A|B)_\rho$ can decrease by at most $\log|Z|$ when conditioning on an additional classical system $Z$, i.e., for any tripartite state $\rho_{ABZ}$ that is classical on $Z$ with respect to some orthonormal basis $\{|z\rangle\}_{z\in\mathcal{Z}}$, we have

$$H(A|BZ)_\rho \geq H(A|B)_\rho - \log|Z| \ . \tag{36}$$

The next lemma can be obtained by applying the asymptotic equipartition property to the corresponding lemma for the smoothed min-entropy in [59]. It shows that the entropy $H(A|BC)_\rho$ cannot increase too much when a projective measurement is applied to system $C$.

*Lemma 8:* Let $\rho_{ABC}$ be a tri-partite state. Furthermore, let $\mathcal{M}$ be a projective measurement in the basis $\{|z\rangle\}_{z\in\mathcal{Z}}$ on C and $\rho_{ABZ} := (\mathbb{1}_{AB} \otimes \mathcal{M})(\rho_{ABC})$. Then,

$$H(A|BC)_\rho \geq H(A|BZ)_\rho - \log|Z| \ .$$

### A. Security Definition

A protocol is an $\varepsilon$-secure implementation of OT in the malicious model if for any adversary $\mathcal{A}$ attacking the protocol (real setting), there exists a *simulator* $\mathcal{S}$ using the ideal OT (ideal setting) such that for all inputs of the honest players the real and the ideal setting can be distinguished with an advantage of at most $\varepsilon$. This definition implies the following three conditions (see also [60]):

- Correctness: If both players are honest, Alice has random inputs $(X_0, X_1) \in \{0,1\}^k \times \{0,1\}^k$ and Bob has input $c \in \{0,1\}$, then Bob always receives $X_c$ in the ideal setting. This implies that in an $\varepsilon$-secure protocol, Bob must output a value $Y$, where

$$\Pr[Y \neq X_c] \leq \varepsilon \ . \tag{37}$$

- Security for Alice: Let Alice be honest and Bob malicious, and let Alice's input be chosen uniformly at random. In the ideal setting, the simulator must provide the ideal OT with a classical input $C' \in \{0,1\}$. He receives the output $Y$ and then outputs a quantum state $\sigma_B$ that may depend on $C'$ and $Y$. The output of the simulator together with classical values $X_0$, $X_1$ and $C'$ now defines the state $\sigma_{X_0X_1BC'}$. Since $X_{1-C'}$ is random and independent of $C'$ and $Y$, we must have

$$\sigma_{X_{1-C'}X_{C'}BC'} = \pi_{\{0,1\}^k} \otimes \sigma_{X_{C'}BC'} \tag{38}$$

and

$$\mathrm{D}(\sigma_{X_0X_1B}, \rho_{X_0X_1B}) \leq \varepsilon \ , \tag{39}$$

[7] Stand-alone statistically secure commitments based on stateless two-party primitives are universally composable [55].

where $\rho_{X_0 X_1 B}$ is the resulting state of the protocol.[8]

- Security for Bob: If Bob is honest and Alice malicious, the simulator outputs a quantum state $\sigma_A$ that is independent of Bob's input $c$. Let $\rho_A^c$ be the state that Alice has at the end of the protocol if Bob's input is $c$. The security definition now requires that $\mathrm{D}(\sigma_A, \rho_A^c) \leq \varepsilon$ for $c \in \{0,1\}$. By the triangle inequality, we get
$$\mathrm{D}(\rho_A^0, \rho_A^1) \leq 2\varepsilon \ . \tag{40}$$

Note that the Conditions (37) - (40) are only necessary for the security of a protocol, they do *not* imply that a protocol is secure.

In the following we present two impossibility results for quantum protocols that implement $\binom{2}{1}$-$\mathsf{OT}^k$ using a bit commitment functionality or randomness distributed to the players. We consider protocols which are information-theoretically secure. In particular, we assume that the adversary has unlimited memory space and can apply arbitrary quantum operations to his whole quantum system. Our proofs use similar techniques as the impossibility results in [37], [38], [39].

We assume that the two parties, Alice and Bob, have access to a noiseless quantum and a noiseless classical channel. The protocol proceeds in rounds, where in any round of the protocol, the parties may perform an arbitrary quantum operation on the system in their possession. This operation can be conditioned on the available classical information and generates the inputs to the communication channels. The quantum channel transfers a part of one party's system to the other party. The classical channel measures the input in a canonical basis and sends the outcome of the measurement to the receiver. We assume that the total number of rounds of the protocol is bounded by a finite number. Since we can always introduce empty rounds, this corresponds to the assumption that the number of rounds is equal in every execution of the protocol.

All quantum operations of both parties can be purified by introducing an additional memory space: Any quantum operation $\mathcal{E}$ can be simulated by adding an ancillary system, applying a unitary on the composite system, and then tracing out part of the remaining system. More precisely, for any TP-CPM $\mathcal{E}$ from $\mathcal{S}_=(\mathcal{H}_\mathrm{A})$ to $\mathcal{S}_=(\mathcal{H}_\mathrm{B})$, there exists a Hilbert space $\mathcal{H}_\mathrm{R}$, a unitary $U$ acting on $\mathcal{H}_{ABR}$ and a pure state $\sigma_{BR} \in \mathcal{S}_=(\mathcal{H}_{BR})$ such that
$$\mathcal{E}(\rho_A) = \mathrm{tr}_\mathrm{AR}(U(\rho_A \otimes \sigma_{BR})U^\dagger). \tag{41}$$
This is known as the *Stinespring dilation* [61] of $\mathcal{E}$. Thus, we can assume that the parties apply in every round of the protocol a unitary to their system conditioned on the information shared over the classical channel. In particular, we can assume that the system remains in a pure state conditioned on the information shared over the classical channel if the initial state of the protocol is pure. Since a malicious player can purify all his quantum operations in the original protocol without being detected, the purified protocol is secure according to our definition if the original protocol is secure.

An important tool in our impossibility proofs is the following technical lemma from [59], which generalizes a result already used in [37], [38], [39].

*Lemma 9:* For $b \in \{0,1\}$, let
$$\rho^b_{XX'AB} = \sum_x P_b(x) |x\rangle\langle x|_X \otimes |x\rangle\langle x|_{X'} \otimes |\psi^{x,b}_{AB}\rangle\langle\psi^{x,b}_{AB}|$$
with $\mathrm{D}(\rho^0_{X'B}, \rho^1_{X'B}) \leq \varepsilon$. Then there exists a unitary $U_{AX}$ such that
$$\mathrm{D}(\rho'^1_{XX'AB}, \rho^1_{XX'AB}) \leq \sqrt{2\varepsilon}$$
where $\rho'^1_{XX'AB} = (U_{XA} \otimes \mathbb{1}_{X'B}) \rho^0_{XX'AB} (U_{XA} \otimes \mathbb{1}_{X'B})^\dagger$.

First, we consider protocols where the players can use a certain number $n$ of ideal bit commitments as a resource to implement an oblivious transfer.

*Theorem 7:* Any protocol that implements a $\binom{2}{1}$-$\mathsf{OT}^k$ with an error of at most $\varepsilon$ , where $0 \leq \varepsilon \leq 0.002$, from black-box bit commitments, has to use at least $(1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon})$ bit commitments.

*Proof:* Let $n_A$ be the number of bit commitments from Alice to Bob and $n_B$ the number of bit commitments from Bob to Alice used in the protocol and $n = n_A + n_B$. Let Alice choose her inputs $X_0$ and $X_1$ uniformly at random. Let the final state of the protocol on Alice's and Bob's system be $\rho^c_{AB}$, when both players are honest and Bob has input $c \in \{0,1\}$. If Bob is executing the protocol honestly using input $c = 1$, he can compute $X_1$ with an error of at most $1 - \varepsilon$. Since the protocol is $\varepsilon$-secure for Alice, we can conclude from Lemma 20 that $\mathrm{D}(\rho^1_{X_0 B}, \tau_{X_0} \otimes \rho^1_B) \leq 5\varepsilon$ . Equation (33) implies that
$$H(X_0|B)_{\rho^1} \geq (1 - 20\varepsilon) \cdot k - 10h(\varepsilon) \ . \tag{42}$$
In the following, we consider a modified protocol that does not use the bit commitment functionality and is not necessarily secure for Alice. In this protocol we make Bob more powerful in the sense that he can simulate the original protocol locally. Thus, the modified protocol is still secure for Bob. Furthermore, the resulting state is pure conditioned on the classical communication. Therefore, we can apply Lemma 9 to derive an upper bound on the entropy of $X_0$ conditioned on Bob's system in the new protocol. Finally, we use the data-processing inequalities for the conditional entropy to show that this entropy can have decreased in the modified protocol by at most the number of commitments, which, together with inequality (33), implies the statement of the theorem.

In the modified protocol, Alice, instead of sending bits to the commitment functionality, measures the bits to be committed, stores a copy of each and sends them to Bob, who stores them in a classical register, $C_A$. When one of these commitments is opened, he moves the corresponding bit to his register $B$. Bob simulates the action of the commitment functionality locally as follows: Instead of measuring a register, $Y$, and sending the outcome to the commitment functionality, he applies the isometry $U : |y\rangle_Y \mapsto |yy\rangle_{YY'}$ purifying the measurement of the committed bit and stores $Y'$ in another register, $C_B$. When

[8] The standard security definition of OT considered here requires Bob's choice bit to be fixed at the end of the protocol. To show that a protocol is insecure, it suffices, therefore, to show that Bob can still choose after the termination of the protocol whether he wants to receive $x_0$ or $x_1$. Lo in [39] shows impossibility of OT in a stronger sense, namely that Bob can learn all of Alice's inputs.

Bob has to open the commitment, he measures $Y'$ and sends the outcome to Alice over the classical channel. The state of the modified protocol is pure conditioned on the classical communication. Let $\rho^c_{ABC}$, where $C$ stands for $C_AC_B$, be the final state of this protocol. Note that its marginal state $\rho^c_{AB}$ is the corresponding state at the end of the original protocol. Since the protocol is $\varepsilon$-secure for Bob, we have $\mathrm{D}(\rho^0_A, \rho^1_A) \leq 2\varepsilon$. From Lemma 9 follows that there exists a unitary $U_{BC}$ such that Bob can transform the state $\rho^1$ into the state $\bar{\rho}^0$ with $\mathrm{D}(\rho^0, \bar{\rho}^0) \leq 2\sqrt{\varepsilon}$. Since given the state $\rho^0_{X_0B}$, $X_0$ can be guessed from $\rho^0_B$ with probability $1-\varepsilon$, it follows from (31) that $X_0$ can be guessed from $\rho^1_{BC}$ with a probability of at least $1-\varepsilon-2\sqrt{\varepsilon}$. By inequality (34), we obtain

$$H(X_0|B)_{\rho^1} \leq h(\varepsilon) + h(2\sqrt{\varepsilon}) + (\varepsilon + 2\sqrt{\varepsilon}) \cdot k \ . \qquad (43)$$

We can use Lemma 8 and inequality (36) to conclude that

$$H(X_0|BC_AC_B)_{\rho^1} \geq H(X_0|B)_{\rho^1} - n \ .$$

For $\varepsilon \leq 0.002$, we have $h(\sqrt{\varepsilon}) > 11h(\varepsilon)$ and $21\varepsilon < \sqrt{\varepsilon}$. This implies the statement. ■

Theorem 7 implies that there exists a constant $c > 0$ such that any protocol that implements $m+1$ bit commitments from $m$ bit commitments must have an error of at least $c/m$, i.e., bit commitment cannot be extended by quantum protocols. This result can be generalized in the following sense: For any protocol that implements a single string commitment from a certain number of bit commitments, the length of the implemented string commitments is essentially bounded by the number of used bit commitments, even if the protocol is allowed to have a small constant error [59].

Next, we consider protocols where the two players have access to distributed randomness $P_{UV}$. We can model this primitive as a quantum primitive $\sum_{u,v} \sqrt{P_{UV}(u,v)} \cdot |u,v\rangle_{UV} \otimes |u,v\rangle_E$ that distributes the values $u$ and $v$ to Alice and Bob and keeps the register $E$.

*Theorem 8:* To implement a $\binom{2}{1}$-$\mathsf{OT}^k$ with an error of at most $\varepsilon$, where $0 \leq \varepsilon \leq 0.002$, from a primitive $P_{UV}$, we need

$$H_{\max}(U|V) + H_{\max}(V|U) \geq (1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon}) \ ,$$

and

$$2H(UV) \geq (1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon}) \ .$$

*Proof:* Let the final state of the protocol on Alice's and Bob's system be $\rho^c_{AB}$, when both players are honest and Bob has input $c \in \{0,1\}$. As in the proof of the previous theorem we have

$$H(X_0|B)_{\rho^1} \geq (1-20\varepsilon) \cdot k - 2h(5\varepsilon) \geq (1-20\varepsilon) \cdot k - 10h(\varepsilon) \ .$$

Consider a modified protocol that starts from a state

$$|\psi\rangle_{UVU'V'} = \sum_{u,v} \sqrt{P_{UV}(u,v)} \cdot |u,v\rangle_{UV} \otimes |u,v\rangle_{U'V'} \ ,$$

where the systems $V$ and $U'V'$ belong to Bob. Again Bob is more powerful in the modified protocol because he can simulate the state of the original protocol locally. As in (43) in the proof of the previous theorem we can, therefore, conclude that

$$H(X_0|BU'V')_{\rho^1} \leq h(\varepsilon) + h(2\sqrt{\varepsilon}) + (\varepsilon + 2\sqrt{\varepsilon}) \cdot k \ .$$

Since measuring register $V'$ and discarding register $U'$ results in the state $\rho^1_{X_0B}$, we can use Lemma 8 and inequality (36) to obtain

$$\begin{aligned} H(X_0|BU'V')_{\rho^1} \geq & H(X_0|B)_{\rho^1} - \max_v \log |\mathrm{supp}(P_{U|V=v})| \\ & - \max_u \log |\mathrm{supp}(P_{V|U=u})| \ . \end{aligned}$$

This implies the first statement. The second statement follows from the inequality

$$H(X_0|BB')_{\rho^1} \geq H(X_0|B)_{\rho^1} - H(B') \ , \qquad (44)$$

which is implied by (35). ■

The theorem immediately implies the following corollary.

*Corollary 12:* To implement a $\binom{2}{1}$-$\mathsf{OT}^k$ with an error of at most $\varepsilon$, where $0 \leq \varepsilon \leq 0.002$, from $n$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ in either direction, we must have

$$2n \geq (1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon}) \ .$$

Theorem 8 implies that $\binom{2}{1}$-$\mathsf{OT}^1$ cannot be extended by quantum protocols in the following sense: Given a protocol that implements $m+1$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ from $m$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ with an error $\varepsilon$, we can apply this protocol iteratively and implement $4m$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ from $m$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ with an error of $\varepsilon' := 3m\varepsilon$, assuming that Bob follows the protocol. Thus, Corollary 12 implies that $12\sqrt{\varepsilon'} + 3h(\sqrt{\varepsilon'})/m \geq 2$ if $\varepsilon' \leq 0.002$. Thus, $\varepsilon' \geq 0.002$ and $\varepsilon \geq \frac{1}{1500m}$. Hence, any quantum protocol that implements $m+1$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ from $m$ instances of $\binom{2}{1}$-$\mathsf{OT}^1$ must have an error of at least $\frac{1}{1500m}$.

The second bound of Theorem 8 also holds for more general primitives that generate a pure state $|\psi\rangle_{ABE}$, distributes registers $A$ and $B$ to Alice and Bob and keeps the purification in its register $E$.

*Theorem 9:* To implement a $\binom{2}{1}$-$\mathsf{OT}^k$ with an error of at most $\varepsilon$, where $0 \leq \varepsilon \leq 0.002$, from a primitive $|\psi\rangle_{ABE}$, we need

$$2H(E)_\psi \geq (1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon}) \ .$$

The proof of Theorem 9 follows exactly the same reasoning as Theorem 8 and is omitted.

Next, we give an additional lower bound for reductions of OT to commitments that shows that the *number* of commitments (of arbitrary size) used in any $\varepsilon$-secure protocol must be at least $\Omega(\log(1/\varepsilon))$. We model the commitments as before, i.e., the functionality applies the isometry $U : |y\rangle_Y \mapsto |yy\rangle_{YY'}$ and stores $YY'$ in separate registers $E_A$ and $E_B$ for Alice and Bob. The proof idea is the following: We let the adversary guess a subset $\mathcal{T}$ of commitments that he will be required to open during the protocol. He honestly executes all commitments in $\mathcal{T}$, but cheats in all others. If the adversary guesses $\mathcal{T}$ right, he is able to cheat in the same way as in any protocol that does not use any commitments.

*Theorem 10:* Any quantum protocol that implements $\binom{2}{1}$-$\mathsf{OT}^k$ using $\kappa$ commitments (of arbitrary length) must have an error of at least $2^{-\kappa}/36$.

*Proof:* We define $\varepsilon := 2^{-\kappa}/36$. Let $\rho^c_{ABE_AE_B}$ be the final state of an $\varepsilon$-secure protocol, when both players are honest and Bob has input $c \in \{0,1\}$. We distinguish two cases. In the first case, we assume that $\mathrm{D}(\rho^0_{AE_A}, \rho^1_{AE_A}) \geq \varepsilon' := 1/18$ . We let Bob be honest and let Alice apply the following strategy: She chooses a random subset $\mathcal{T}$ of $[k]$. She executes all commitments in $\mathcal{T}$ honestly, but for all commitments not in $\mathcal{T}$ she sends $|0\rangle$ to $E_A$ and simulates the action of the commitment functionality in her quantum register. Otherwise, she follows the whole protocol honestly.

During the execution of the protocol, Bob may ask Alice to open a certain set of commitments, $\mathcal{T}'$. If $\mathcal{T}' = \mathcal{T}$, which happens with probability $2^{-\kappa}$ independently of everything else, then at the end of the protocol the global state is $\rho^c$, but $E_A$ is now part of Alice's system. Thus, the states of Alice's system for $c = 0$ and $c = 1$, have distance at least $\varepsilon' \cdot 2^{-\kappa} > 2\varepsilon$, which contradicts condition (40).

In the second case, we assume that $\mathrm{D}(\rho^0_{AE_A}, \rho^1_{AE_A}) < \varepsilon'$. From condition (37) follows that honest Bob can guess $X_1$ with probability $1 - \varepsilon$ if $c = 1$. According to Lemma 20, $X_0$ should be $5\varepsilon$-close to uniform with respect to $\rho^1_B$. To obtain a contradiction to the security condition (39), it is according to equation (32) sufficient to show that Bob can guess the first bit of $X_0$ with a probability greater than $1/2 + 5\varepsilon$.

Again, if Bob guesses the set $\mathcal{T}$ right, then $E_B$ is part of Bob's system. Then Lemma 9 guarantees the existence of a unitary $U_{BE_B}$ such Bob can transform the state $\rho^1$ into a state $\bar\rho^1$ with $\mathrm{D}(\rho^0, \bar\rho^1) \leq \sqrt{2\varepsilon'}$. Thus, Bob can guess $X_0$ with an error of at most $\sqrt{2\varepsilon'} + \varepsilon$ given $\bar\rho^1$. If he fails to guess $\mathcal{T}$, he simply outputs a random bit as his guess for the first bit of $X_0$. Since the probability that he guesses the subset $\mathcal{T}$ correctly is exactly $2^{-\kappa}$, he can guess the first bit of $X_0$ with probability

$$\begin{aligned}(1-2^{-\kappa}) \cdot \frac{1}{2} &+ 2^{-\kappa} \cdot (1 - \varepsilon - \sqrt{2\varepsilon'}) \\ &= \frac{1}{2} + 2^{-\kappa} \cdot \left(\frac{1}{2} - \varepsilon - \sqrt{2\varepsilon'}\right) \\ &> \frac{1}{2} + 2^{-\kappa} \cdot \left(\frac{1}{2} - \varepsilon'/2 - \sqrt{2\varepsilon'}\right) \\ &= \frac{1}{2} + 2^{-\kappa} \cdot \frac{5}{36} \\ &= \frac{1}{2} + 5\varepsilon \ .\end{aligned}$$

■

## VI. Reduction of OT to String Commitments

We will now show how to construct a protocol that is optimal with respect to the lower bounds of both Theorem 7 and Theorem 10.

We modify the protocol from [24] by grouping the $m$ pairs of values into $\kappa$ blocks of size $b := m/\kappa$. We let Bob commit to the blocks of $b$ pairs of values at once. The subset $\mathcal{T}$ is now of size $\alpha\kappa$, and defines the blocks to be opened by Bob. If Bob is able to open all commitments in $\mathcal{T}$ correctly, then the state of the protocol must be close in a certain sense to the state that would result from correctly measuring all qubits. Since we consider security in the malicious model, a dishonest player may abort the protocol by not sending any message. A possibility to handle this would be to include a special output `aborted` to the definition of the primitive. Here, we take the following, different approach, which is also used, for example, in [62]: Whenever a player does not send a (well-formed) message, the other player assumes that a fixed default message as, for example, the all-zero string has been sent. Note that our protocol is different from the protocols analyzed in [26], [63]. Besides replacing the bit commitments by strings commitments, Alice outputs two random strings if Bob aborts in the commitment or in the check step. This allows us to implement an ideal OT functionality that does not have a special output `aborted`.

Protocol **OTfromCommitment**

1) Alice prepares $m$ EPR pairs, $(|00\rangle + |11\rangle)/\sqrt{2}$, and sends one qubit of each pair to Bob. Bob selects $\hat\theta \in \{0,1\}^m$ at random and measures the received qubits in basis $\hat\theta$, obtaining $\hat x \in \{0,1\}^m$. Alice chooses a basis $\theta \in \{0,1\}^m$ at random (but does not measure her qubits yet).
2) Bob commits in blocks of size $b$ to $\hat\theta$ and $\hat x$. Alice samples a random subset $t \subseteq [\kappa]$ of cardinality $\alpha\kappa$ and asks Bob to open the commitments to the corresponding blocks of values $(\hat\theta_i, \hat x_i)$. Let $\mathcal{T}$ be the set of bits in $[m]$ corresponding to $t$. Alice measures her qubits indexed by $\mathcal{T}$ in Bob's basis $\hat\theta_t$ to obtain $x_t$ and verifies that $x_i = \hat x_i$ whenever $\theta_i = \hat\theta_i$. If Bob does not commit to all values as required or does not open all commitments or if Alice detects an inconsistency, Alice outputs outputs two random $k$-bit strings $z_0, z_1$ and terminates the protocol.
3) (Set partitioning) Alice sends $\theta$ to Bob. Bob partitions $\bar{\mathcal{T}} := [m] \setminus \mathcal{T}$ into the subsets $I_c = \{i \in \bar{\mathcal{T}} : \ \theta_i = \hat\theta_i\}$ and $I_{1-c} = \{i \in \bar{\mathcal{T}} : \ \theta_i \neq \hat\theta_i\}$ and sends $I_0$ and $I_1$ to Alice. Additionally, Alice measures her qubits in basis $\theta$ to obtain $x$.
4) (Key extraction) Alice chooses and sends to Bob two-universal hash functions $f_0, f_1$ with output length $k$, and computes $z_0 := f_0(x_{I_0})$ and $z_1 := f_1(x_{I_1})$. Bob computes $z_c = f(\hat x_{I_0})$.

We only need to estimate the error probability of the classical sampling strategy that corresponds to the new checking procedure of Alice and apply the result from [63]. We need the following sampling result, which follows from Lemma 5.5 in [64] and Hoeffding's inequality [65].

*Lemma 10:* Let $\alpha \in [0, \frac{1}{2}]$. Let $y = (y_1, \ldots y_m)$ be a bit string of length $m := b\kappa$ that we group into $\kappa$ blocks of size $b$. Let $t$ be a random subset of $[\kappa]$ of size $\alpha\kappa$, $\mathcal{T}$ the corresponding set of bits in $[m]$ and $\bar{\mathcal{T}}$ the complement of $\mathcal{T}$. Let $\mathcal{T}'$ be a random subset of $\mathcal{T}$, where every element is chosen to be in $\mathcal{T}'$ with probability $\frac{1}{2}$, independently of everything else. We have for any $\delta > 0$

$$\Pr\left[\frac{1}{|\mathcal{T}'|}\sum_{i\in\mathcal{T}'} y_i \le \frac{1}{(1-\alpha)m}\sum_{i\in\bar{\mathcal{T}}} y_i - \delta\right] \le \varepsilon\ ,$$

where $\varepsilon := 3\exp(-(1/2-\varepsilon)\alpha\kappa\delta^2/8$.

*Lemma 11 (Security for Alice):* Let $Z_0$ and $Z_1$ be the strings from $\{0,1\}^k$ output by Alice. Then there exists a binary $C$ such that for any $\varepsilon, \delta > 0$ the following upper bound on the distance from uniform of $Z_{1-C}$ with respect to $Z_C$ and Bob's system holds:

$$\begin{aligned}\mathrm{D}(\rho_{Z_{1-C}Z_C EC}, \tau_{\{0,1\}^k}{\otimes}\rho_{Z_C EC}) & \\ \le 2^{-\frac{1}{2}((\frac{1}{4}-\varepsilon/2-h(\delta))(1-\alpha)m-k)-1} & \\ + 2\exp(-2\varepsilon^2(1-\alpha)m) & \\ + \sqrt{3}\exp(-\alpha'\kappa\delta^2/16)\ , & \qquad (45)\end{aligned}$$

where $E$ denotes the quantum state output by Bob, $\mathbb{1}$ the identity operator on $\mathbb{C}^{2^k}$ and $\alpha' := (1/2-\delta)\alpha$.

*Proof:* We consider the state shared between Alice and Bob after Bob has committed to the bases $\hat{\theta}$ and the measurement outcomes $\hat{x}$ where we can assume $\hat{\theta} = \hat{x} = (0,\dots,0)$. Since we want to prove an upper bound on (45), we can assume that Bob always opens all commitments. Otherwise the distance from uniform can only decrease. Alice now chooses a subset $\mathcal{T}$ to be opened by Bob. As in the proof of Theorem 4 from [66], Lemma 10 implies that the joint state is $\sqrt{3}\exp(-\alpha'\kappa\delta^2/16)$-close to an ideal state that is for every choice of $\mathcal{T}$ and $\mathcal{S}$ in a superposition of states with relative Hamming weight in a $\delta$-neighbourhood of $\beta$ within $A_{\bar{\mathcal{T}}}$, where $\beta$ is the number of inconsistencies that Alice detects and $\mathcal{S}$ is the subset of $\mathcal{T}$ that Alice checks. We assume that the state equals this ideal state and add the error later. Then, following the proof of Theorem 4 in [63] for $\beta = 0$, we obtain that the distance from uniform of one of the outputs with respect to Bob's system (given the other output) is bounded from above by

$$2^{-\frac{1}{2}((\frac{1}{4}-\varepsilon/2-h(\delta))(1-\alpha)m-k)-1} + 2\exp(-2\varepsilon^2(1-\alpha)m)\ .$$

If $\beta > 0$, the distance from uniform is zero. Thus, the statement follows by adding the distance of the ideal state to the real state. ■

*Lemma 12 (Security for Bob):* The protocol is perfectly secure for Bob.

*Proof:* Let $\rho_{A'YC}$ be the state created by the protocol if Bob is honest. We consider a hypothetical protocol where Bob does not use any commitments. He stores all the qubits received from Alice. After Alice sends the set $\mathcal{T}$, he chooses a basis $\hat{\theta}$ and measures his qubits corresponding to $\mathcal{T}$ to obtain $\hat{x}_{\mathcal{T}}$ in basis $\theta$, but does not yet measure the other qubits. Then he sends $\hat{x}_{\mathcal{T}}$ and $\hat{\theta}_{\mathcal{T}}$ to Alice. After he gets the basis $\theta$ from Alice he measures all his remaining qubits in Alice's basis $\theta$ to obtain $\hat{x}_{\bar{\mathcal{T}}}$. Next, he chooses his input $C \in \{0,1\}$ and constructs the sets $I_0$ and $I_1$ using $\theta$ and $\hat{\theta}$ as in the protocol. After receiving $f_0, f_1 \in \mathcal{F}$ from Alice, he computes $z_0 = f_0(\hat{x}_{I_0})$ and $z_1 = f_1(\hat{x}_{I_1})$ . This results in a state $\sigma_{A'Z_0Z_1C}$, where $Z_0$ and $Z_1$ are the values computed by Bob. We have $\sigma_{A'Z_0Z_1C} = \sigma_{A'Z_0Z_1} \otimes \sigma_C$ and $\sigma_{A'Z_CC} = \rho_{A'YC}$. ■

*Lemma 13 (Correctness):* The protocol is perfectly correct.

*Proof:* If both players are honest, then $Z_0$, $Z_1$ and $C$ are independently distributed according to the required distributions. Furthermore, Bob always computes $Z_C$ as his output. ■

The following theorem is then immediately implied by Lemmas 11, 12 and 13.

*Theorem 11:* There exists a quantum protocol that uses $\kappa = O(\log 1/\varepsilon)$ commitments of size $b$, where $\kappa b = O(k + \log 1/\varepsilon)$, and implements a $\binom{2}{1}$-$\mathsf{OT}^k$ with an error of at most $\varepsilon$.

## VII. Conclusions

## References

[1] S. Winkler and J. Wullschleger, "On the efficiency of classical and quantum oblivious transfer reductions," in *CRYPTO*, ser. Lecture Notes in Computer Science, vol. 6223. Springer, 2010, pp. 707–723.

[2] A. C. Yao, "Protocols for secure computations," in *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '82)*, 1982, pp. 160–164.

[3] O. Goldreich and R. Vainish, "How to solve any protocol problem - an efficiency improvement," in *Advances in Cryptology — CRYPTO '87*, ser. Lecture Notes in Computer Science. Springer-Verlag, 1988, pp. 73–86.

[4] J. Kilian, "Founding cryptography on oblivious transfer," in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*. ACM Press, 1988, pp. 20–31.

[5] M. O. Rabin, "How to exchange secrets by oblivious transfer," Harvard Aiken Computation Laboratory, Tech. Rep. TR-81, 1981.

[6] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Commun. ACM*, vol. 28, no. 6, pp. 637–647, 1985.

[7] C. Crépeau, "Equivalence between two flavours of oblivious transfers," in *Advances in Cryptology — EUROCRYPT 1987*, ser. Lecture Notes in Computer Science. Springer-Verlag, 1988, pp. 350–354.

[8] G. Brassard, C. Crépeau, and J.-M. Robert, "Information theoretic reductions among disclosure problems," in *Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science (FOCS '86)*, 1986, pp. 168–173.

[9] C. Crépeau and M. Sántha, "On the reversibility of oblivious transfer," in *Advances in Cryptology — EUROCRYPT '91*, ser. Lecture Notes in Computer Science, vol. 547. Springer, 1991, pp. 106–113.

[10] G. Brassard, C. Crépeau, and M. Santha, "Oblivious transfers and intersecting codes," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1769–1780, 1996.

[11] Y. Dodis and S. Micali, "Lower bounds for oblivious transfer reductions," in *Advances in Cryptology — EUROCRYPT '99*, ser. Lecture Notes in Computer Science, vol. 1592. Springer-Verlag, 1999, pp. 42–55.

[12] S. Wolf and J. Wullschleger, "New monotones and lower bounds in unconditional two-party computation." in *Advances in Cryptology — CRYPTO '05*, ser. Lecture Notes in Computer Science, vol. 3621, 2005, pp. 467–477.

[13] C. Crépeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions (extended abstract)," in *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science (FOCS '88)*, 1988, pp. 42–52.

[14] C. Crépeau, K. Morozov, and S. Wolf, "Efficient unconditional oblivious transfer from almost any noisy channel." in *Proceedings of Fourth Conference on Security in Communication Networks (SCN)*, ser. Lecture Notes in Computer Science, vol. 3352. Springer-Verlag, 2004, pp. 47–59.

[15] I. Damgård, S. Fehr, K. Morozov, and L. Salvail, "Unfair noisy channels and oblivious transfer." in *Theory of Cryptography Conference — TCC '04*, ser. Lecture Notes in Computer Science, vol. 2951. Springer-Verlag, 2004, pp. 355–373.

[16] J. Wullschleger, "Oblivious transfer from weak noisy channels," in *Theory of Cryptography*, ser. Lecture Notes in Computer Science, O. Reingold, Ed. Springer Berlin / Heidelberg, 2009, vol. 5444, pp. 332–349.

[17] S. Wolf and J. Wullschleger, "Zero-error information and applications in cryptography," in *Proceedings of 2004 IEEE Information Theory Workshop (ITW '04)*, 2004.

[18] A. Nascimento and A. Winter, “On the oblivious transfer capacity of noisy correlations,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT ’06)*, 2006.

[19] C. Cachin, “On the foundations of oblivious transfer,” in *Advances in Cryptology — EUROCRYPT ’98*, ser. Lecture Notes in Computer Science, vol. 1403. Springer-Verlag, 1998, pp. 361–374.

[20] I. Damgård, J. Kilian, and L. Salvail, “On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions,” in *Advances in Cryptology — EUROCRYPT ’99*, ser. Lecture Notes in Computer Science, vol. 1592. Springer-Verlag, 1999, pp. 56–73.

[21] G. Brassard, C. Crépeau, and S. Wolf, “Oblivious transfers and privacy amplification,” *Journal of Cryptology*, vol. 16, no. 4, pp. 219–237, 2003.

[22] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, “Oblivious transfer and linear functions,” in *Advances in Cryptology — CRYPTO ’06*, ser. Lecture Notes in Computer Science, vol. 4117. Springer-Verlag, 2006.

[23] J. Wullschleger, “Oblivious-transfer amplification,” in *Advances in Cryptology - EUROCRYPT 2007*, ser. Lecture Notes in Computer Science, M. Naor, Ed. Springer Berlin / Heidelberg, 2007, vol. 4515, pp. 555–572.

[24] C. H. Bennett, G. Brassard, C. Crépeau, and H. Skubiszewska, “Practical quantum oblivious transfer,” in *Advances in Cryptology — CRYPTO ’91*, ser. Lecture Notes in Computer Science, vol. 576. Springer, 1992, pp. 351–366.

[25] A. C.-C. Yao, “Security of quantum protocols against coherent measurements,” in *Proceedings of the 27th Annual ACM Symposium on Theory of Computing (STOC ’95)*. ACM Press, 1995, pp. 67–75.

[26] I. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner, “Improving the security of quantum protocols,” in *Advances in Cryptology — CRYPTO ’09*, ser. Lecture Notes in Computer Science. Springer-Verlag, 2009.

[27] D. Unruh, “Universally composable quantum multi-party computation,” in *Advances in Cryptology EUROCRYPT 2010*, ser. Lecture Notes in Computer Science, H. Gilbert, Ed. Springer Berlin / Heidelberg, 2010, vol. 6110, pp. 486–505.

[28] D. Beaver, “Correlated pseudorandomness and the complexity of private computations,” in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC ’96)*. ACM Press, 1996, pp. 479–488.

[29] U. Maurer, “Information-theoretic cryptography,” in *Advances in Cryptology CRYPTO 99*, ser. Lecture Notes in Computer Science, M. Wiener, Ed. Springer Berlin / Heidelberg, 1999, vol. 1666, pp. 785–785.

[30] S. Wolf and J. Wullschleger, “New monotones and lower bounds in unconditional two-party computation.” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2792–2797, 2008.

[31] V. Prabhakaran and M. Prabhakaran, “Assisted common information,” in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, june 2010, pp. 2602 –2606.

[32] ——, “Assisted common information: Further results,” in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, 31 2011-aug. 5 2011, pp. 2861 –2865.

[33] K. Kurosawa, W. Kishimoto, and T. Koshiba, “A combinatorial approach to deriving lower bounds for perfectly secure oblivious transfer reductions,” *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2566 –2571, june 2008.

[34] A. Beimel and T. Malkin, “A quantitative approach to reductions in secure computation,” in *Theory of Cryptography*, ser. Lecture Notes in Computer Science, M. Naor, Ed., vol. 2951. Springer Berlin / Heidelberg, 2004, pp. 238–257.

[35] C. Crépeau and G. Savvides, “Optimal reductions between oblivious transfers using interactive hashing,” in *Advances in Cryptology — EUROCRYPT ’06*, ser. Lecture Notes in Computer Science, vol. 4004. Springer-Verlag, 2006, pp. 201–221.

[36] R. Ahlswede and I. Csiszar, “On oblivious transfer capacity,” ISIT, 2007, 2007.

[37] D. Mayers, “Unconditionally secure quantum bit commitment is impossible,” *Physical Review Letters*, vol. 78, pp. 3414–3417, 1997.

[38] H. K. Lo and H. F. Chau, “Is quantum bit commitment really possible?” *Physical Review Letters*, vol. 78, pp. 3410–3413, 1997.

[39] H. K. Lo, “Insecurity of quantum secure computations,” *Physical Review A*, vol. 56, p. 1154, 1997.

[40] L. Salvail, C. Schaffner, and M. Sotáková, “On the power of two-party quantum cryptography,” in *ASIACRYPT*, ser. Lecture Notes in Computer Science, M. Matsui, Ed., vol. 5912. Springer, 2009, pp. 70–87.

[41] G. Brassard, C. Crépeau, and M. Sántha, “Oblivious transfers and intersecting codes,” *IEEE Transactions on Information Theory, special issue on coding and complexity*, vol. 42, no. 6, pp. 1769–1780, 1996.

[42] G. Savvides, “Interactive hashing and reductions between oblivious transfer variants,” Ph.D. dissertation, McGill University, Montreal, 2007.

[43] Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in *EUROCRYPT*, ser. Lecture Notes in Computer Science, C. Cachin and J. Camenisch, Eds., vol. 3027. Springer, 2004, pp. 523–540.

[44] R. Renner, “Security of quantum key distribution,” Ph.D. dissertation, ETH Zurich, Switzerland, 2005, available at arxiv.org/abs/quant-ph/0512258.

[45] N. Nisan and D. Zuckerman, “Randomness is linear in space,” *J. Comput. Syst. Sci.*, vol. 52, pp. 43–52, February 1996.

[46] R. Renner and S. Wolf, “Simple and tight bounds for information reconciliation and privacy amplification,” in *Advances in Cryptology — ASIACRYPT 2005*, ser. Lecture Notes in Computer Science, vol. 3788. Springer-Verlag, 2005, pp. 199–216.

[47] D. Beaver, “Precomputing oblivious transfer,” in *Advances in Cryptology — EUROCRYPT ’95*, ser. Lecture Notes in Computer Science, vol. 963. Springer-Verlag, 1995, pp. 97–109.

[48] O. Goldreich, *Foundations of Cryptography*. Cambridge University Press, 2004, vol. II: Basic Applications.

[49] M. Fitzi, S. Wolf, and J. Wullschleger, “Pseudo-signatures, broadcast, and multi-party computation from correlated randomness,” in *Advances in Cryptology — CRYPTO ’04*, ser. Lecture Notes in Computer Science, vol. 3152. Springer-Verlag, 2004, pp. 562–578.

[50] P. Gacs and J. Körner, “Common information is far less than mutual information,” *Probl. Contr. Inform. Theory*, vol. 2, pp. 149–162, 1973.

[51] S. Wolf and J. Wullschleger, “Oblivious transfer is symmetric,” in *Advances in Cryptology — EUROCRYPT ’06*, ser. Lecture Notes in Computer Science, vol. 4004. Springer-Verlag, 2006, pp. 222–232.

[52] S. Winkler, “Classical and quantum secure two-party computation,” Ph.D. dissertation, ETH Zurich, 2012.

[53] L. Salvail, C. Schaffner, and M. Sotáková, “On the power of two-party quantum cryptography,” arXiv:0902.4036, 2009.

[54] R. Canetti, “Universally composable security: A new paradigm for cryptographic protocols,” in *Proceedings of the 42th Annual IEEE Symposium on Foundations of Computer Science (FOCS ’01)*, 2001, pp. 136–145, updated Version available at http://eprint.iacr.org/2000/067.

[55] R. Dowsley, J. van de Graaf, J. Mller-Quade, and A. C. A. Nascimento, “On the composability of statistically secure bit commitments,” Cryptology ePrint Archive, Report 2008/457, 2008.

[56] A. Winter, A. C. A. Nascimento, and H. Imai, “Commitment capacity of discrete memoryless channels.” in *IMA Int. Conf.*, 2003, pp. 35–51.

[57] R. Alicki and M. Fannes, “Continuity of quantum conditional information,” *Journal of Physics A: Mathematical and General*, vol. 37, no. 5, p. L55, 2004.

[58] H. Araki and E. H. Lieb, “Entropy inequalities,” *Comm. Math. Phys.*, vol. 18, pp. 160–170, 1970.

[59] S. Winkler, M. Tomamichel, S. Hengl, and R. Renner, “Impossibility of growing quantum bit commitments,” *Phys. Rev. Lett.*, vol. 107, p. 090502, Aug 2011.

[60] S. Fehr and C. Schaffner, “Composing quantum protocols in a classical environment,” in *Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography*, ser. TCC ’09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 350–367.

[61] W. F. Stinespring, “Positive functions on $C^*$-algebras,” *Proc. Amer. Math. Soc.*, vol. 6, pp. 211–216, 1955.

[62] R. Konig, S. Wehner, and J. Wullschleger, “Unconditional security from noisy quantum storage,” *Information Theory, IEEE Transactions on*, vol. 58, no. 3, pp. 1962 –1984, march 2012.

[63] N. Bouman and S. Fehr, “Sampling in a quantum population, and applications,” arXiv:0907.4246v4, 2009.

[64] L. Babai and T. P. Hayes, “Near-independence of permutations and an almost sure polynomial bound on the diameter of the symmetric group,” SODA ’05, 2005.

[65] W. Hoeffding, “Probability inequalities for sums of bounded random variables,” *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963.

[66] N. J. Bouman and S. Fehr, “Sampling in a quantum population, and applications,” in *CRYPTO*, ser. Lecture Notes in Computer Science, vol. 6223. Springer, 2010, pp. 724–741.

[67] M. Prabhakaran and M. Rosulek, “Cryptographic complexity of multi-party computation problems: Classifications and separations,” in *Advances in Cryptology CRYPTO 2008*, ser. Lecture Notes in Computer Science, D. Wagner, Ed. Springer Berlin / Heidelberg, 2008, vol. 5157, pp. 262–279.

# Appendix

## A. Malicious OT implies Semi-honest OT

In the malicious model the adversary is not required to follow the protocol. Therefore, a protocol that is secure in the malicious model protects against a much bigger set of adversaries. On the other hand, the security definition in the malicious model only implies that for any (also semi-honest) adversary there exists a *malicious* simulator for the ideal primitive, i.e., the simulator is allowed to change his input or output from the ideal primitive. Since this is not allowed in the semi-honest model, security in the malicious model does not imply security in the semi-honest model in general. For implementations of OT[9], however, it has been shown in [67] that this implication *does* hold, because if the adversary is semi-honest, a simulator can only change the input with small probability. Otherwise, he is not able to correctly simulate the input or the output of the protocol. Therefore, any impossibility result for OT in the semi-honest model also implies impossibility in the malicious model.

We will state these result for $\binom{n}{1}$-$\mathsf{OT}^k$ with explicit bounds on the errors.

*Lemma A.1:* If a protocol implementing $\binom{n}{1}$-$\mathsf{OT}^k$ is secure in the malicious model with an error of at most $\varepsilon$, then it is also secure in the semi-honest model with an error of at most $(2n+1)\varepsilon$.

*Proof:* From the security of the protocol we know that there exists a (malicious) simulator that simulates the view of honest Alice. If two honest players execute the protocol on input $(x_0, \ldots, x_{n-1})$ and $c$, then with probability $1-\varepsilon$ the receiver gets $y = x_c$. Thus, the simulator can change the input $x_i$ with probability at most $2\varepsilon$ for all $0 \leq i < n-1$. We construct a new simulator that executes the malicious simulator but never changes the input. This simulation is $(2n+1)\varepsilon$-close to the distribution of the protocol. From the security of the protocol we also know that there exists a (malicious) simulator that simulates the view of honest Bob. If two honest players execute the protocol with uniform input $(X_0, \ldots, X_{n-1})$ and choice bit $c$, then with probability $1-\varepsilon$ the receiver gets $y = x_c$. If the simulator changes the choice bit $c$, he does not learn $x_c$ and the simulated $y$ is not equal to $x_c$ with probability at least $1/2$. Therefore, the simulator can change $c$ or the output with probability at most $4\varepsilon$. As above we can construct a simulator for the semi-honest model with an error of at most $5\varepsilon$. ■

Note that some of our proofs could easily be adapted to the malicious model to get slightly better bounds than the ones that follow from the combination of the bounds in the semi-honest model and Lemma A.1.

## B. Smooth Entropies

In the following we prove different properties of the entropies $H^\varepsilon_{\min}(X|Y)$ and $H^\varepsilon_{\max}(X|Y)$. Note that some of these properties (or special cases of them) have already been shown in [46].

We first introduce the following auxiliary quantities.

*Definition 6:* For random variables $X, Y$ and $\varepsilon \in [0,1)$, we define

$$r^\varepsilon_{\max}(X|Y) := \min_{\Omega:\Pr[\Omega]\geq 1-\varepsilon} \max_{y\in\mathcal{Y}} |\text{supp}\,(P_{X\Omega|Y=y})| \text{ and}$$

$$r^\varepsilon_{\min}(X|Y) := \min_{\Omega:\Pr[\Omega]\geq 1-\varepsilon} \sum_{y\in\mathcal{Y}} P_Y(y) \max_x P_{X\Omega|Y=y}(x) \ .$$

Note that $H^\varepsilon_{\min}(X|Y) = -\log r^\varepsilon_{\min}(X|Y)$ and $H^\varepsilon_{\max}(X|Y) = \log r^\varepsilon_{\max}(X|Y)$.

The following lemma shows that the smooth conditional max-entropy is subadditive.

*Lemma 14 (Subadditivity):* Let $X, Y, Z$ be random variables and $\varepsilon, \varepsilon' \geq 0$ such that $\varepsilon + \varepsilon' \in [0,1)$. Then

$$H^{\varepsilon+\varepsilon'}_{\max}(XY|Z) \leq H^\varepsilon_{\max}(X|Z) + H^{\varepsilon'}_{\max}(Y|XZ) \ .$$

*Proof:* Let $\Omega$ be an event with $\Pr[\Omega] \geq 1-\varepsilon$ and

$$\max_{x,z} |\text{supp}\,(P_{Y\Omega|X=x,Z=z})| \leq r^\varepsilon_{\max}(Y|XZ) \ .$$

Let $\Omega'$ be an event with $\Pr[\Omega'] \geq 1-\varepsilon'$ and $\Omega' \leftrightarrow (X,Z) \leftrightarrow (Y,\Omega)$ such that

$$\max_z |\text{supp}\,(P_{X\Omega'|Z=z})| \leq r^\varepsilon_{\max}(X|Z) \ .$$

Then $\Pr[\Omega, \Omega'] \geq 1-\varepsilon-\varepsilon'$ and

$$r^{\varepsilon+\varepsilon'}_{\max}(XY|Z) \leq \max_z |\text{supp}\,(P_{XY\Omega\Omega'|Z=z})| \ .$$

We have

$$\begin{aligned}
&\max_z |\text{supp}\,(P_{XY\Omega\Omega'|Z=z})| \\
&\quad\leq \max_z (|\text{supp}\,(P_{X\Omega'|Z=z})| \cdot \max_x |\text{supp}\,(P_{Y\Omega|X=x,Z=z})|) \\
&\quad\leq \max_z |\text{supp}\,(P_{X\Omega'|Z=z})| \cdot \max_{x,z} |\text{supp}\,(P_{Y\Omega|X=x,Z=z})| \ .
\end{aligned}$$

■

Next, we show that conditioning on an additional random variable cannot reduce the conditional smooth entropies.

*Lemma 15:* Let $X, Y, Z$ be random variables and $\varepsilon \in [0,1)$. Then

$$H^\varepsilon_{\min}(X|Z) \geq H^\varepsilon_{\min}(X|YZ) \ .$$

*Proof:* Let $\Omega$ be an event with $\Pr[\Omega] \geq 1-\varepsilon$. Then

$$\begin{aligned}
&\sum_z P_Z(z) \max_x P_{X\Omega|Z=z}(x) \\
&\qquad= \sum_z P_Z(z) \max_x \sum_y P_{Y|Z=z}(y) P_{X\Omega|Y=y,Z=z}(x) \\
&\qquad\leq \sum_z P_Z(z) \max_{x,y} P_{X\Omega|Y=y,Z=z}(x) \ .
\end{aligned}$$

■

The Shannon entropy satisfies the inequality $H(X|Z) - H(X|YZ) = I(X;Y|Z) \leq H(Y|Z)$. The next lemma shows that this property can be generalized to the smooth min- and max-entropy.

*Lemma 16:* Let $X, Y, Z$ be random variables and $\varepsilon, \varepsilon' \geq 0$ such that $\varepsilon + \varepsilon' \in [0,1)$. Then

$$H^\varepsilon_{\min}(X|Z) - H^{\varepsilon'}_{\max}(X|YZ) \leq H^{\varepsilon+\varepsilon'}_{\min}(Y|Z) \ .$$

[9] And any other so-called deviation revealing functionality.

*Proof:* Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$ and

$$\sum_z \max_x P_{XZ\Omega}(x, z) \leq r^{\varepsilon}_{\min}(X|Z) \ .$$

Let $\Omega'$ be an event with $\Pr[\Omega'] \geq 1 - \varepsilon'$ such that

$$\max_{y,z} |\text{supp}\,(P_{X\Omega'|Y=y,Z=z})| \leq r^{\varepsilon}_{\max}(X|YZ) \ .$$

Then $\Pr[\Omega, \Omega'] \geq 1 - \varepsilon - \varepsilon'$ and

$$r^{\varepsilon+\varepsilon'}_{\min}(Y|Z) \leq \sum_z P_Z(z) \max_y P_{Y\Omega\Omega'|Z=z}(y) \ .$$

We have for all $z$

$$\begin{aligned} \max_{x,y} P_{XY\Omega\Omega'|Z=z}(x, y) &\leq \max_{x,y} P_{XY\Omega|Z=z}(x, y) \\ &\leq \max_x P_{X\Omega|Z=z}(x) \ . \end{aligned}$$

Furthermore, we have

$$|\{x : P_{XY\Omega\Omega'|Z=z}(x, y) > 0\}| \leq |\text{supp}\,(P_{X\Omega'|Y=y,Z=z})| \ .$$

Together, we obtain

$$\begin{aligned} r^{\varepsilon+\varepsilon'}_{\min}(Y|Z) &\leq \sum_z P_Z(z) \max_y P_{Y\Omega\Omega'|Z=z}(y) \\ &= \sum_z P_Z(z)(\max_y \sum_x P_{XY\Omega\Omega'|Z=z}(x, y)) \\ &\leq \sum_z P_Z(z)(\max_{y,z} |\text{supp}\,(P_{X\Omega\Omega'|Y=y,Z=z})| \\ &\qquad \cdot \max_{x,y} P_{XY\Omega\Omega'|Z=z}(x, y)) \\ &\leq \max_{y,z} |\text{supp}\,(P_{X\Omega'|Y=y,Z=z})| \\ &\qquad \cdot \sum_z P_Z(z) \max_x P_{X\Omega|Z=z}(x) \\ &\leq r^{\varepsilon}_{\min}(X|Z) \cdot r^{\varepsilon'}_{\max}(X|YZ) \ . \end{aligned}$$

■

Note that the proof also implies the stronger inequality $H^{\varepsilon}_{\min}(XY|Z) - H^{\varepsilon'}_{\max}(X|YZ) \leq H^{\varepsilon+\varepsilon'}_{\min}(Y|Z)$, which corresponds in a certain sense to the inequality $H(X|Z) - H(X|YZ) \leq H(XY|Z)$ for the Shannon entropy.

The following lemma shows that the smooth min-entropy $H^{\varepsilon}_{\min}(X|Y)$ satisfies a data processing inequality, i.e., it cannot be decreased by additionally processing $Y$.

*Lemma 17 (Data Processing):* Let $X, Y, Z$ be random variables with $X \leftrightarrow Y \leftrightarrow Z$ and $\varepsilon \in [0, 1)$. Then

$$H^{\varepsilon}_{\min}(X|Y) \leq H^{\varepsilon}_{\min}(X|YZ) \ .$$

*Proof:* Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$ and $\Omega \leftrightarrow XY \leftrightarrow Z$ such that

$$r^{\varepsilon}_{\min}(X|Y) = \sum_y P_Y(y) \max_x P_{X\Omega|Y=y}(x) \ .$$

We have

$$\begin{aligned} P_{X\Omega|Y=y,Z=z}(x) &= P_{X|Y=y,Z=z}(x) P_{\Omega|X=x,Y=y,Z=z} \\ &= P_{X|Y=y}(x) P_{\Omega|X=x,Y=y} \\ &= P_{X\Omega|Y=y}(x) \ . \end{aligned}$$

Thus, we obtain

$$\begin{aligned} r^{\varepsilon}_{\min}(X|YZ) &\leq \sum_{y,z} P_{YZ}(y, z) \max_x P_{X\Omega|Y=y,Z=z}(x) \\ &= \sum_y P_Y(y) \max_x P_{X\Omega|Y=y}(x) \ . \end{aligned}$$

■

The smooth max-entropy $H^{\varepsilon}_{\max}(X|Y)$ also satisfies a data processing inequality, i.e., it cannot be decreased by additionally processing $Y$.

*Lemma 18:* Let $X, Y, Z$ be random variables with $X \leftrightarrow Y \leftrightarrow Z$ and $\varepsilon \in [0, 1)$. Then

$$H^{\varepsilon}_{\max}(X|Y) \leq H^{\varepsilon}_{\max}(X|YZ) \ .$$

*Proof:* Let $\Omega$ be an event such that

$$r^{\varepsilon}_{\max}(X|YZ) = \max_{y,z} |\text{supp}\,(P_{X\Omega|Y=y,Z=z})| \ .$$

For all $y$, we define $\varepsilon_y := P_{\Omega|Y=y}$. Let $\Omega_y$ be an event such that

$$r^{\varepsilon_y}_{\max}(X|Z, Y = y) = \max_z |\text{supp}\,(P_{X\Omega_y|Y=y,Z=z})| \ .$$

Let $\bar{z}_y$ be such that $P_{\Omega_y|Y=y,Z=\bar{z}}$ is maximal. We define $\bar{\Omega}_y$ with $P_{\bar{\Omega}_y|X=x,Y=y} := P_{\Omega_y|X=x,Y=y,Z=\bar{z}}$. Then, we have $P_{\bar{\Omega}_y|Y=y} \geq P_{\Omega_y|Y=y} \geq 1 - \varepsilon_y$ and $P_{X\Omega_y|Y=y,Z=z} \geq P_{X\Omega_y|Y=y,Z=\bar{z}} = P_{X\bar{\Omega}_y|Y=y}$ and, therefore,

$$r^{\varepsilon_y}_{\max}(X|Z, Y = y) \geq r^{\varepsilon_y}_{\max}(X|Y = y) \ .$$

Thus, we get

$$\begin{aligned} r^{\varepsilon}_{\max}(X|YZ) &= \max_{y,z} |\text{supp}\,(P_{X\Omega|Y=y,Z=z})| \\ &\geq \max_y r^{\varepsilon_y}_{\max}(X|Z, Y = y) \\ &\geq \max_y r^{\varepsilon_y}_{\max}(X|Y = y) \\ &\geq r^{\varepsilon}_{\max}(X|Y) \ . \end{aligned}$$

■

The smooth max-entropy satisfies the following monotonicity properties.

*Lemma 19:* Let $X, Y, Z$ be random variables and $\varepsilon \in [0, 1)$. Then

$$H^{\varepsilon}_{\max}(XY|Z) \geq H^{\varepsilon}_{\max}(X|Z) \geq H^{\varepsilon}_{\max}(X|YZ) \ .$$

*Proof:* Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$. Then the first inequality follows from

$$\max_z |\text{supp}\,(P_{XY\Omega|Z=z})| \geq \max_z |\text{supp}\,(P_{X\Omega|Z=z})| \ .$$

and the second inequality from

$$\max_{y,z} |\text{supp}\,(P_{X\Omega|Y=y,Z=z})| \leq \max_z |\text{supp}\,(P_{X\Omega|Z=z})| \ .$$

■

### C. *Technical Lemmas*

Lemma 1. Let $(X, Y)$ and $(\hat{X}, \hat{Y})$ be random variables distributed according to $P_{XY}$ and $P_{\hat{X}\hat{Y}}$, and let $\mathrm{D}(P_{XY}, P_{\hat{X}\hat{Y}}) \leq$

$\epsilon$. Then

$$H(\hat{X}|\hat{Y}) \geq H(X|Y) - \epsilon \log |\mathcal{X}| - \mathrm{h}(\epsilon) \ .$$

*Proof:* There exist random variables $A, B$ such that $P_{XY|A=0} = P_{\hat{X}\hat{Y}|B=0}$ and $\Pr[A=0] = \Pr[B=0] = 1-\epsilon$. Thus, using the monotonicity of the entropy and the fact that $H((|X)) \leq \log |\mathcal{X}|$ we get that

$$\begin{aligned} H(\hat{X}|\hat{Y}) &\geq (1-\varepsilon) H(\hat{X}|\hat{Y}A=0) + \varepsilon H(\hat{X}|\hat{Y}A=1) \\ &\geq (1-\epsilon) H(X|YB=0) \\ &= H(X|YB) - \epsilon H(X|YB=1) \\ &= H(XB|Y) - H(B|Y) - \epsilon H(X|YB=1) \\ &\geq H(X|Y) - \mathrm{h}(\epsilon) - \epsilon \log |\mathcal{X}| \ . \end{aligned}$$

■

*Lemma 20:* Let $\rho_{X_0X_1B}$ satisfy conditions (38) and (39). If there exists a measurement $G$ on system $B$ such that $\Pr[G(\rho_B) = X_1] \geq 1-\varepsilon$, then

$$\mathrm{D}(\rho_{X_0X_1B}, \tau_{X_0} \otimes \rho_{X_1B}) \leq 5\varepsilon \ .$$

*Proof:* Let $\sigma_{X_0X_1BC'}$ be the state in conditions (38) and (39). Then (32) implies

$$\Pr[G(\sigma_B) = X_1] \geq \Pr[G(\rho_B) = X_1] - \varepsilon \geq 1 - 2\varepsilon \ .$$

In the state $\sigma_{X_0X_1BC'}$, we can guess the first bit of $X_{1-C'}$ if we output the first bit of $G(\sigma^B)$ whenever $C'=0$ and a random bit otherwise. We succeed with a probability of

$$\begin{aligned} g \geq& \frac{1}{2} \cdot \Pr[C'=1] + \Pr[G(\sigma^B) = X_1 \wedge C'=0] \\ =& \frac{1}{2} \cdot (1 - \Pr[C'=0]) + \Pr[C'=0] \\ & \quad - \Pr[G(\sigma^B) \neq X_1 \wedge C'=0] \\ \geq& \frac{1}{2} \cdot (1 - \Pr[C'=0]) + \Pr[C'=0] - 2\varepsilon \\ =& \frac{1}{2} + \frac{\Pr[C'=0]}{2} - 2\varepsilon \ . \end{aligned}$$

Since $X_{1-C'}$ is uniform with respect to the rest, we have $g \leq \frac{1}{2}$ and, therefore, $\Pr[C'=0] \leq 4\varepsilon$. This implies that for $\hat{\sigma}_{X_0X_1BC'} := \tau_{X_0} \otimes \sigma_{X_1B} \otimes |1\rangle\langle 1|$ we have

$$\mathrm{D}(\sigma_{X_{1-C'}X_{C'}BC'}, \hat{\sigma}_{X_{1-C'}X_{C'}BC'}) \leq 4\varepsilon$$

and hence

$$\begin{aligned} \mathrm{D}(\rho_{X_0X_1B}, \tau_{X_0} \otimes \rho_{X_1B}) \leq& \ \mathrm{D}(\rho_{X_0X_1B}, \sigma_{X_0X_1B}) \\ & + \mathrm{D}(\sigma_{X_0X_1B}, \hat{\sigma}_{X_0X_1B}) \\ \leq& \ 5\varepsilon \ . \end{aligned}$$

■